PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : A63F

A2

(11) International Publication Number: **WO 99/01188**

(43) International Publication Date: 14 January 1999 (14.01.99)

(21) International Application Number: PCT/US98/13909

(22) International Filing Date: 2 July 1998 (02.07.98)

(30) Priority Data:
08/888,049 3 July 1997 (03.07.97) US

(71) Applicant: WALKER ASSET MANAGEMENT LIMITED PARTNERSHIP [US/US]; 5 High Ridge Park, Stamford, CT 06905–1325 (US).

(72) Inventors: WALKER, Jay, S.; 124 Spectacle Lane, Ridgefield, CT 06877 (US). SCHNEIER, Bruce; 101 East Minnehaha Parkway, Minneapolis, MN 55419 (US). JORASCH, James, A.; Apartment 5G, 25 Forest Street, Stamford, CT 06901 (US). VAN LUCHENE, Andrew, S.; 13–2A Clarmore Drive, Norwalk, CT 06850 (US).

(74) Agent: ANDERSON, Jay, H.; Fitzpatrick, Cella, Harper & Scinto, 30 Rockefeller Plaza, New York, NY 10112–3801 (US).

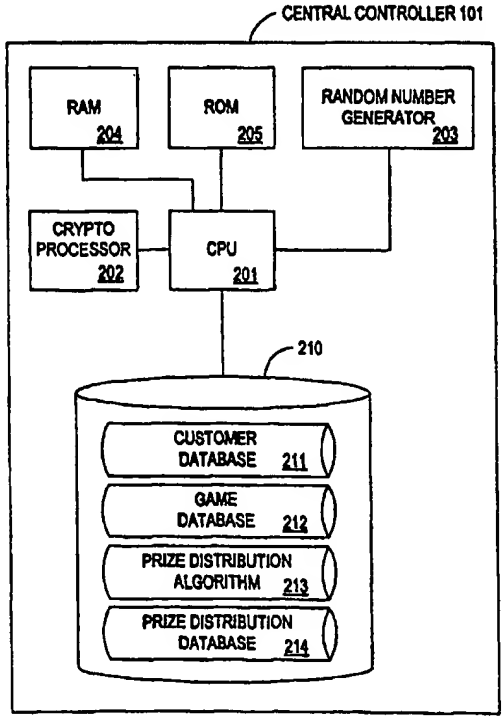
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD AND APPARATUS FOR SECURING ON-LINE VIRTUAL PUNCHBOARD TRANSACTIONS

(57) Abstract

A system is described for facilitating an Internet–based game of chance, particularly a computer–based version of a punchboard game having a grid with prizes associated with the various grid locations. The user can pay a central controller for each selection by providing a credit card number, or through other Internet transaction means. The central controller sends the user a fresh virtual punchboard (i.e. a game in which no selections have yet been made). The user selects a grid location, encrypts it, and then transmits it to the central controller. The central controller then generates prize values for the grid that it sent to the player. The user's computer stores the locations of each prize and determines whether the player's selection was a winner. If he has won, the player sends the decryption key to the central controller to decrypt his grid selection and authenticate his selection. The central controller then initiates a payment to the user.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

TITLE

METHOD AND APPARATUS FOR SECURING ON-LINE VIRTUAL PUNCHBOARD TRANSACTIONS

BACKGROUND OF THE INVENTION

This invention relates to an electronic gambling game in which a player selects from a series of possible outcomes. The player and game provider may interact in a variety of ways, including over the Internet.

A number of well-known gambling games are based on a player selecting from a series of possible outcomes, where the winning outcome is randomly generated using some physical or mechanical device furnished by the game operator. Examples of such games are roulette, slot machines, and bingo. In the classical embodiments of these games, the player sees and/or hears the outcome generated (as in bingo and roulette), or even has a hand in generating the outcome himself (as in slot machines). The player's trust in the fairness of these games (that is, his belief that the outcome is random and that his selection, if a winner, will be honored) is largely based on his personal observation. Similarly, the game operator can use various methods to prevent cheating by a player if the player is

personally present; for example, a bingo player claiming to be a winner is required to offer his card for inspection.

A well-known example of an entertainment/gambling device is the "punchboard." A punchboard consists of a board with a square grid of holes. Each hole contains a small rolled-up piece of paper. The player takes a pin and pushes through the board, pushing a selected piece of paper through the other side. This paper is then unrolled by the player to reveal whether or not he has won a prize. In a typical punchboard game, a player pays a small sum (approximately $1) to make a selection; prizes are determined by the size of the board and the fees, and may run hundreds of dollars.

Here, too, the player's confidence in the fairness of the game is largely based on his observation of the board; since he selects a piece of paper and can immediately read the message on it, he can be sure that the paper is not switched or tampered with after he selects it. In addition, by watching a number of plays he can eventually satisfy himself that there are indeed winning locations somewhere on the board. A successful electronic version of a punchboard game (a "virtual punchboard") must offer the player similar assurance that the game is not rigged, and must also prevent cheating the player.

Various forms of electronic games of chance have been available for many years. The way these games are played, however, is changing dramatically with the use of digital computers operating on electronic networks such as the Internet. Players can now connect to a remote server and wager electronically. Rather than traveling to the game (casino, bingo hall, etc.), a player can log into an electronic game and wager from

the comfort of his own home. While this remote playing has many advantages, it raises several security issues. In a typical electronic gambling game, the player enters his selection and then learns whether he has won, without observing the winning selection being generated. For example, when playing card games at a casino, a player can observe the dealer shuffle and deal the cards and thus has some confidence that the outcome was generated randomly. In an electronic casino, the shuffling process is typically digitally generated, driven by random number generators which the player cannot see. The player cannot know whether the random number generated is truly random or was selected by the casino to give it an advantage.

Furthermore, a player desiring to play an electronic game remotely (for example, communicating with a game provider on the Internet) must send his selection and receive the winning selection over a communication network. In this instance, both the player and game provider require assurance that the communications are secure and that the game is conducted fairly.

Electronic game providers have tried to increase players' confidence in the legitimacy of games by assuring players that gaming software has not been tampered with. For example, an electronic game provider may allow an independent third party to perform an audit of the software. This is a time-consuming and expensive process, however. With complex software running into the hundreds of thousands of lines of code, it is very difficult to find a few lines of code that alter the randomness of the outcomes. Also, use of an independent, third party auditor shifts the need for trust to another party, and does not guarantee the legitimacy of the game.

Some electronic lottery systems have used methods for securing communications between remote player terminals and a central controller. For example, U.S. Patent No. 4,652,998 to Koza et al. ("Video Gaming System With Pool Prize Structures") describes cryptographic methods for securing these communications. In games dependent on the use of random numbers, however, simply securing against the transmission of a fraudulent random number does not solve the problem of assuring the player that the game is fairly conducted. Nor does it solve the problem of preventing multiple players from cooperating to gain an advantage over the game provider.

U.S. Patent No. 5,326,104 to Pease et al. ("Secure Automated Electronic Casino Gaming System") describes a system whereby a number of keno playing devices, all within the same playing area, are connected to a central controller. A player can play a device by inserting a player account card into it which is registered and confirmed by the central controller. Security in this system is directed primarily to ensuring that players will not tamper with the keno terminals, and that employees will not enter false tickets into the system. Apparently it is assumed that the central controller is trusted and will not try to cheat the players.

U.S. Patent No. 5,569,082 to Kayer ("Personal Computer Lottery Game") describes a game whereby a player can purchase a game piece containing an encrypted code which determines whether the piece is a winning one. The player logs onto a central site, via a PC or a kiosk, and types in the code. The site runs a game which reveals to the player if he is a winner in "an exciting fashion." If the player is a winner, he will be given instructions by the site as to where to pick up his prize. Although the system described in this

patent provides encryption to protect the site from fraud, it offers no encryption to protect the player.

U.S. Patent No. 5,547,202 to Tsumura ("Computer Game Device") describes a system whereby a player can pay for the usage of games transmitted to his PC or to a kiosk via satellite from a central controller. The games are scrambled until payment is made. The central controller can store a game so that a player can take breaks from a game, return to it and continue play from the point in the game at which he left it. This system has neither a gambling element nor is it cryptographically enabled.

U.S. Patent No. 5,269,521 to Rossides ("Expected Value Payment Method and System For Reducing the Expected Per Unit Costs of Paying and/or Receiving a Given Amount of Commodity") describes a system where a customer exchanges encoded numbers with a product vendor. After being decoded, the two numbers are combined to determine a result. (See column 30, lines 1 to 5, as well as column 30, line 35, to column 31, line 55). The transactions described are not conducted in an online manner. Additionally, both parties must encode their numbers before exchanging them. No game results are ever exchanged in encoded form.

U.S. Patent No. 4,309,569 to Merkle ("Method of providing digital signatures") describes a system for digital signatures utilizing hash trees.

The proliferation of electronic network technology, along with the ease of user access to networks such as the Internet, has dramatically increased electronic communications and the exchange of information. Among a myriad of other uses, these networks facilitate the playing of games, including gambling activities. They

are particularly well suited for such gaming because of their ability to collapse geographic distances while linking distributed players. As discussed above, however, the electronic implementation of games, and particularly gambling activities, often results in the loss of confidence and validity otherwise imbued in players from their personal observation of traditional gaming procedures (for example, dealing cards, spinning roulette wheels, etc.).

There thus exists a need in the art for systems and procedures which can both actually and in the perception of players improve the security and operation of electronic gambling and games. Such systems and procedures would not only foster the perception of on-line gaming as legitimate, but also increase player participation in such activities. This would further increase the commercial value of what is already a substantial online business.

SUMMARY OF THE INVENTION

In accordance with the present invention there is provided a new and improved method and apparatus for facilitating computer-based games of chance on electronic networks such as the Internet. A key feature of the invention comprises the use of encoding techniques, including various encryption schemes, to validate the operation of the games and prevent cheating by either the player or the game provider. Although encryption methods are described, it should be noted that any encoding scheme which prevents the recipient of a message from deciphering its contents will suffice.

In accordance with one embodiment of the invention, a method of generating and verifying the results of a computer-based game of chance is implemented by transmitting to a player computer a plurality of available game selections, each identified by a unique selection identifier. A player selection identifier is received from the player computer, and a winning selection identifier transmitted to the player computer. The player selection identifier and the winning selection identifier are compared to determine if the player has won the game. In accordance with the invention, verification is made that the winning selection identifier and the player selection identifier were independently generated.

Game operation is preferably managed by a central controller, with players communicating with the controller through player computers connected over an electronic network. In different embodiments of the invention, verification of authenticity is provided in the central controller, the player computer, some combination of both, or with the involvement of a third party.

Games supported include all games of chance which permit a user to select from amongst a plurality of potentially winning selections. Applicable games include, but are not limited to a punchboard having punch locations, a roulette wheel having wheel numbers, a bingo game having user-selected card numbers, and a slot machine having user-selectable outcomes.

Verification is provided through a variety of techniques, including the use of encryption such as key-based encryption, and hash-based encryption. The invention further contemplates the use of a third-party

trusted agent to monitor and verify that the player and winning selections were independently generated.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram showing an overview of the system of the present invention.

Figure 2 is a block diagram of the central controller of Figure 1.

Figure 3 is a block diagram of the user computer of Figure 1.

Figure 4 is a block diagram of a trusted third party computer.

Figure 5 is a schematic representation of the punchboard game area before a game has been played.

Figure 6 is a schematic representation of the punchboard game area after a game has been played.

Figure 7A shows in tabular form the fields of the customer database of the central controller.

Figure 7B shows in tabular form the information in the prize distribution database of the central controller.

Figure 8 is a flowchart describing initiation of a game according to the preferred embodiments of the present invention.

Figure 9A shows in tabular form the information in the audit database of the user computer according to the first embodiment of the invention.

Figure 9B shows in tabular form the information in the game database of the central controller according to the first embodiment of the invention.

Figures 10A and 10B are connected flowcharts describing the flow of play between the central controller and user computer according to the first embodiment of the invention.

Figure 11A shows in tabular form the information in the audit database of the user computer according to the second embodiment of the invention.

Figure 11B shows in tabular form the information in the game database of the central controller according to the second embodiment of the invention.

Figures 12A and 12B are connected flowcharts describing the flow of play between the user computer and the central controller according to the second embodiment of the invention.

Figure 13A shows in tabular form the information in the audit database of the user computer according to the third embodiment of the invention.

Figure 13B shows in tabular form the information in the game database of the central controller according to the third embodiment of the invention.

Figures 14A, 14B and 14C are connected flowcharts describing the flow of play between the user computer and the central controller according to the third embodiment of the invention.

Figure 15A shows in tabular form the information in the audit database of the user computer according to the fourth embodiment of the invention.

Figure 15B shows in tabular form the information in the game database of the central controller according to the fourth embodiment of the invention.

Figure 16 is a flowchart describing the flow of play between the user computer and the central controller according to the fourth embodiment of the invention.

Figure 17A shows in tabular form the information in the audit database of the third party according to the fifth embodiment of the invention.

Figure 17B shows in tabular form the information in the game database of the central controller according to the fifth embodiment of the invention.

Figures 18A and 18B are connected flowcharts describing the flow of play between the user computer, the central controller, and the third party computer according to the fifth embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

An overview of the system in the preferred embodiments of the present invention is shown in Figure 1. The central controller 101, operated by the game provider, communicates with the user computer 102 (operated by the game player) over the Internet 100. Figure 2 is a schematic diagram of the structure of the central controller 101. The central controller includes a CPU 201, connected to a cryptoprocessor 202, a random number generator 203, RAM 204, ROM 205 and a data

storage device 210. The CPU 201 connects to the Internet for communication with the player's computer. The data storage device 210 includes a customer database 211, a game database 212, storage for the prize distribution algorithm 213 and a prize distribution database 214. To perform the various functions described in more detail below, the CPU 201 executes a program or programs stored in RAM 204 and/or ROM 205.

Cryptographic processor 202 supports the encoding and decoding of communications with players, as well as the authentication of players. An MC68HC16 microcontroller, commonly manufactured by Motorola Inc., may be used for cryptographic processor 202. This microcontroller utilizes a 16-bit multiply-and-accumulate instruction in the 16 MHZ configuration and requires less than one second to perform a 512-bit private key operation. Other exemplary commercially available specialized cryptographic processors include VLSI Technology's 33MHz 6868 or Semaphore Communications' 40 MHZ Roadrunner 284. Alternatively, cryptographic processor 202 may be configured as part of CPU 201.

A conventional random number generating processor may be used for random number generator 203. The HEMT integrated circuit manufactured by Fujitsu, for example, is capable of generating over one billion random numbers per second. Alternatively, random number generator 203 may be incorporated into CPU 201. Data storage device 210 may include hard disk, magnetic, or optical storage units, as well as CD-ROM drives or flash memory.

The user computer 102 is shown schematically in Figure 3. The user computer includes a CPU 301, connected to

a cryptoprocessor 302, a random number generator 303, RAM 304, ROM 305 and a data storage device 310. The CPU 301 is also connected to an input device 320 and to the Internet, for communication with the user and the central controller respectively. In addition, the CPU 301 is connected to a display device 330 for displaying a virtual punchboard to the user. The data storage device 310 includes an audit database 311. The CPU 301, cryptoprocessor 302, random number generator 303 and data storage device 310 may have the same features as CPU 201, cryptoprocessor 202, random number generator 203 and data storage device 210 discussed just above.

Figure 4 is a schematic diagram of a trusted third party computer 400, which is used in an embodiment of the invention discussed in more detail below. This computer includes a CPU 401, RAM 404, ROM 405 and data storage device 410, similar to central controller 101 and user computer 102. The data storage device includes an audit database 411. The CPU 401 is connected for communication with the user computer 102 and the central controller 101.

Figure 5 shows the appearance of a virtual punchboard display 500, displayed to a user on the display device 330, before a game is played. The game is identified by a number 510, and an empty grid 511 is shown (in this case, a 12 x 12 square). A box 512 appears where the player may enter his selected grid locations. The player's current credits 513 (how much he has paid for the present game, plus his winnings so far) may also be displayed; in the example shown, the player has no winning balance and has just made an electronic payment of $1 to play game # 6465484564.

Figure 6 shows a results display 600, similarly displayed to the user by display device 330, after the game is played. The winning locations are displayed in a table 610 and on the grid 611, with the player's selection circled on the grid and displayed in a box 612. Also displayed is the result of the game (in this case the player is told, "YOU WIN!") and the balance 613 of the player's winnings. Finally, the display includes a box 620 labeled "PLAY AGAIN?" The CPU 301 may advantageously execute interactive display software (stored in RAM 304 or ROM 305) which enables "click boxes" and the like. In that case, the player would click on the "PLAY AGAIN?" box to order a new game.

Figure 7A shows the fields of the customer database 211 maintained by the central controller 101. Each customer is identified by name 701 and is assigned an ID number 702. Each customer entry in the database also includes a credit card number 703, the customer's e-mail address 704 and postal mailing address 705, the total amount the customer has spent 706, and the customer's total winnings to that point 707. The database stores the grid selection preferences 708 for each customer (so that a player who regularly plays the same location on the grid need not enter that location in every game), and the customer's preferred method 709 of receiving his winnings.

The fields of the prize distribution database 214, maintained by the central controller 101, are shown in Figure 7B. Each prize distribution is assigned an identification number 711. Each entry in the database includes the size 712 of the grid, the denomination of the game 713 (that is, the cost to the customer for one play) and the number and amount of prizes 714 to be awarded. Generally, a larger grid has more prizes

associated therewith, and a grid with larger prizes has a larger associated denomination.

To create a new game, the central controller 101 employs a prize distribution algorithm 213 having the following steps: The central controller 101 retrieves the prize structure 714 and grid size 712 from the prize distribution database 214 by searching for the prize distribution ID number 711. The CPU 201 instructs the random number generator 203 to produce enough random numbers to cover the number of grid locations for the game. Each random number is appended to a grid location. The format might be (x,y,r), where "x" is the x-coordinate of the grid location, "y" is the y-coordinate of the grid location, and "r" is the assigned random number. The random numbers are then ranked numerically. Prizes are then appended to each grid location. The format might be (x,y,r,p), with "p" the prize value (which may be zero) assigned to the grid location (x,y). The game is then assigned an ID number. The winning grid locations for the game, and the prizes associated with those locations, are then stored in the game database 212, detailed embodiments of which are described below. Those skilled in the art will appreciate that there are many possible algorithms by which the prices may be randomly assigned. The above algorithm is merely illustrative

First Embodiment (User Computer Encryption)

In the first embodiment of the invention, the fields of the audit database 311 (stored in the user computer 102) are as shown in Figure 9A. Each record in the audit database 311 corresponds to one game played by the user, and is filled in as the game progresses (as described in detail below). A record includes an identification number 901 for the game, the grid

location or locations 902 selected by the player, the winning grid locations 903, the game denomination 713, and a random key 904 which the player uses to encrypt his grid location selections.

In this embodiment, the fields of the game database 212 (stored in the central controller 101) are as shown in Figure 9B. Each record in the game database corresponds to one game (having an ID number 901) played by one player (having an ID number 702). Each record includes the winning grid locations 903, the player's selected and encrypted grid location 910, the corresponding decrypted grid location 920, and the player key 904.

A game conducted according to the first embodiment of the invention begins with the steps shown in the flowchart of Figure 8. Initially, the player (using his computer 102) logs on to the central controller 101 via the Internet 100 (step 801). If the player does not yet have an account (that is, an entry in the customer database 211), an account is opened at this time; the player provides the necessary information (step 804), and the central controller 101 assigns him an ID number and stores the new record in the customer database 211 (step 805). If the player already has an account, he enters his customer ID number 702 (step 810).

The player then selects the amount of money he wishes to play--that is, the denomination of the game; for example, $1, $3, or $5 (step 820). The user computer 102 updates the denomination field 713 in the audit database 311 (step 830). The central controller 101 debits the credit card account of the player for the amount of money played (step 840). The central controller 101 retrieves a new game grid from the prize distribution database 214 (step 850). Using the prize

distribution algorithm 213 described above, the central controller 101 generates the winning grid locations 903, assigns the game identification number 901 and stores the game in the game database 212 (step 860).

In this embodiment, the game continues with the steps shown in the flowcharts of Figures 10A and 10B. In step 1001 of Figure 10A, a "blank" punchboard 500 including the game identification number 510 is made available to the player. The player selects a grid location 902 and enters it into the user computer 102 using input device 320 (step 1002). The cryptographic processor 302 of the user computer 102 generates a player key 904, preferably based on a random number generated by random number generator 303 (step 1003). The cryptographic processor 302 encrypts the grid location selection 902 with the player key (step 1004). The user computer 102 stores the game identification number, player key, and grid location selection in the audit database 311 (step 1005).

In step 1006, the encrypted grid location and game identification number are transmitted to the central controller 101. The central controller then retrieves the record in the game database 212 corresponding to the game identification number received from the user computer 102 (step 1007). The central controller 101 stores the encrypted grid location 910 in the game database 212 (step 1008).

At this point, the central controller 101 has the player's grid location selection, but only in an encrypted form. The central controller 101 then transmits the winning grid locations 903 to the user computer 102 (step 1010 of Figure 10B).

If the player has not won, he may proceed to select a new game (step 1061). If the player has won, the user computer 102 transmits the player key 904 and game identification number to the central controller 101 (step 1051). The central controller decrypts the encrypted grid location 910, and stores the decryption result 920 (the player's selected, winning grid location) and player key 904 in the game database 212 (step 1052).

The amount of money won by the player is retrieved from winning grid location field 903 of the game database 212 (step 1053). The central controller 101 then sends the game result message 600 to the user computer 102, indicating that the player has won (step 1054). The central controller then proceeds to generate the next game (step 1055).

At the end of the billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1056). If money is due the customer, the central controller 101 initiates a payment to the customer according to the customer's preferred payment method 709 (step 1057).

It should be noted that a key element of this embodiment is that the user sends his grid location selection in encrypted form (thus unreadable by the central controller 101) to the central controller before receiving the winning grid locations. The player is thereby assured that the game provider cannot change the winning locations based upon knowledge of his selection. On the other hand, the central controller holds the player's encrypted selection before the player is given the winning locations, and the player must provide the key to decrypt his selection before the central controller awards him a

prize. The encryption of the player's selection thus assures both parties that the game has been fairly conducted, and that the two numbers were independently generated.

A transmission between the central controller and the player may include a digital signature to provide further assurance of the authenticity of the transmission, and to prevent repudiation by the sender. The uses and advantages of digital signatures are discussed generally in Schneier, "Applied Cryptography" (2d ed. 1996), chapter 2.

The above embodiment is also applicable to a game such as roulette. Instead of encoding his grid location selection, the player encrypts his number selection (representing any of the 38 wheel slots). The central controller then transmits the result of the wheel spin to the player.

The game of bingo could be simulated as follows. The player selects a board and then encrypts his selection before sending it to the central controller. The central controller then sends out each bingo number until one of the players claims a win. The winning player sends his key to the central controller so that his selection can be verified.

To simulate a slot machine, the player simply selects one of the possible reel combinations of the slot machine. In a slot machine with three reels and 20 stops per reel, there are 8,000 (20 X 20 X 20) possible outcomes, so the player could select one of these at random, encrypting the selection and sending it to the central controller. The central controller then distributes the prizes among the possible outcomes and

sends the complete set of outcomes to the player so that he can determine whether or not he has won.

Second Embodiment (One-Way Hash)

In the second embodiment of the invention, the audit database 311 in the user computer 102 has a structure as shown in Figure 11A. As in the first embodiment, each record in the audit database corresponds to one game. A record includes the game identification number 901, selected grid location or locations 902, winning grid locations 903 and the game denomination 713, similar to the record shown in Figure 9A. In this embodiment, the record also includes the hash value 1101 of the winning grid locations 903.

The structure of the game database 212 in this embodiment is shown in Figure 11B. Each entry in the game database has a game identification number 901, a customer identification number 702 and the winning grid locations 903, as in the first embodiment. The entry also has the user-selected grid location 902 and the hash value 1101 of the winning grid locations 903.

A game conducted according to the second embodiment of the invention begins with the steps shown in the flowchart of Figure 8 as already described above, and continues with the steps shown in the flowcharts of Figures 12A and 12B. In step 1201 of Figure 12A, the cryptoprocessor 202 of the central controller 101 retrieves the winning grid locations 903 of the game from the game database 212, and uses a one-way hash function to hash the winning grid locations 903, thereby generating the hash value 1101. The hash value 1101 represents a one-way transformation of the winning grid locations 903.

An important feature of the one-way hash function is that it is computationally simple (given the hash function) to generate the hash value, but computationally unfeasible to recreate the winning grid locations from the hash value alone. The hash value 1101 thus serves as a unique identifier for the winning grid locations 903, without the winning grid locations themselves being revealed. Further details on one-way hash functions are given in Schneier, "Applied Cryptography" (2d ed. 1996), chapter 18.

The central controller 101 distributes the hash value 1101 to the user computer 102, along with a "blank" punchboard 500 with game identification number 510 (step 1202). The user computer 102 stores the hash value and game ID number in the audit database 311 (step 1203). In step 1204, the player selects a grid location and enters it into the user computer 102; the player may make additional grid location selections. Once the player has made all of his selections, the user computer 102 stores the game identification number 901, the selected grid locations 902 and the hash value 1101 in the audit database 311 (step 1211). The user computer 102 transmits the selected grid locations 902 to the central controller 101 along with the game ID number (step 1212). It should be noted that at this point the central controller 101 has the player's selections, but has already provided the player with a representation of the winning grid locations in the form of the hash value 1101. In step 1213, the central controller 101 determines whether the player has chosen a winning grid location by comparing the selected locations 902 with the winning grid locations 903 for that game.

Referring now to Figure 12B, the central controller 101 sends the winning grid locations 903 to the user

computer 102 (step 1251). In step 1252, the user computer 102 verifies the fairness of the game. Specifically, the cryptographic processor 302 of the user computer 102 applies the one-way hash function to the received winning grid locations to verify that the hash value 1101 given to him before sending his selection is equal to the new hash value calculated by applying the one-way hash function to the winning grid locations.

If the player has not won, the central controller 101 proceeds to generate the next game (step 1270). If the player has won, the central controller 101 updates the total money awarded 707 in the customer database 211 to reflect the amount the player has just won (step 1260), and then generates the next game. In addition, at the end of a billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1280). If money is due the player, the central controller 101 initiates a payment to the customer according to customer's payment method preference 709 (step 1281).

It should be noted that in this embodiment the punchboard cannot be reused; it must be replaced with a fresh punchboard after each player selection. If the punchboard were not replaced, the player could continue to select grid locations after receiving the winning grid locations 903 (see step 1251). The player could, however, make more than one selection during a game session (see step 1204), as long as each selection was received by the central controller 101 before the winning locations were transmitted to the player.

With minor modifications, this embodiment of the invention can accommodate any number of players. By delaying the transmission of the winning grid locations

until after all grid location selections have been received, any number of players can be accommodated with one punchboard. Alternatively, games could be conducted at great speed, preventing players from cheating by sharing winning locations. For example, two players might make selections on the same punchboard nearly simultaneously. The first player sends his grid location selection and then receives the winning grid locations. A fraction of a second later the second player sends his grid location selection. If the first player can communicate with the second player he can inform the second player of the winning grid locations, ensuring a win for the second player. If the time difference between the two plays is small enough, however, the first player will not have enough time to communicate the winning locations.

Third Embodiment (Hash Tree)

The third embodiment of the invention uses hash trees to accommodate multiple players in a single punchboard game. Details of hash tree techniques are well known in the art and for reference purposes are discussed in Merkle (U.S. Patent No. 4,309,569).

In this embodiment, each grid location is represented by $(x,y,p,h_{xy'})$, where x and y are the coordinates, p is the prize associated with that location, h_{xy} is the hash value of that location, and $h_{xy'}$ is an aggregate hash value for all the other locations. Furthermore, a hash value, h, is calculated for the entire grid (including all locations) using hash function H. This function has the property $H(h) = H(h_{xy},h_{xy'})$ That is, the hash value for the entire grid is equal to the hash value of one location combined with the locations's $h_{xy'}$ value. For additional security, a random number may be

attached to each grid location to provide greater variation in the resulting hash values.

In this embodiment of the invention, the audit database 311 in the user computer 102 has a structure as shown in Figure 13A. As in the previous embodiments, each record in the audit database corresponds to one game. A record includes the game identification number 901, selected grid location or locations 902, winning grid locations 903 and the game denomination 713, similar to the records shown in Figures 9A and 11A. In this embodiment, the record also includes the hash value 1101 for all grid locations (both winning and losing), and an aggregate hash value 1301, representing the hash value of the aggregate of all the grid locations not selected by the player (i.e. the h_{xy} values of all the grid locations selected by the player).

The structure of the game database 212 in this embodiment is shown in Figure 13B. Each entry in the game database has a game identification number 901, a customer identification number 702 and the winning grid locations 903, as in the previous embodiments. The entry also has the user-selected grid location 902, the denomination 713 of the game, the hash value 1101 for all grid locations, and the aggregate hash value 1301.

A game conducted according to the third embodiment of the invention begins with the steps shown in the flowchart of Figure 8 as already described above, and continues with the steps shown in the flowcharts of Figures 14A, 14B and 14C.

In step 1401, the cryptoprocessor 202 of the central controller 101 retrieves the value of all grid locations of the game from the game database 212, and uses one-way hash function H stored in the memory (RAM

204 or ROM 205) of the central controller to hash these grid locations, thereby generating h, the hash value 1101 (i.e. the hash value of all grid locations). The central controller 101 then (step 1402) distributes the hash value 1101 to the user computer 102, along with a "blank" punchboard 500 including the game identification number 510. The user computer 102 stores the hash value 1101 in the audit database 311 (step 1403). The player selects a grid location 902 and enters it into the user computer 102, using the input device 320 (step 1404). The player may enter additional selections if he so desires. After the player has made all of the selections for that game, a new record is entered in the audit database 311 of the user computer 102, reflecting the ID number for the game and the player's selected grid locations (step 1410). The user computer 102 then transmits the player's grid selections 902 and game ID number to the central controller 101 along with the game ID number (step 1411).

The central controller then (step 1451) queries the game database 212 to obtain the winning grid locations 903, to determine whether or not the player's grid selections correspond to the winning grid locations. The central controller 101 sends a message to the user computer 102 relating whether the player has won (step 1452).

The integrity of the game is verified in steps 1453 through 1457. Using the hash tree algorithm, the cryptoprocessor 202 of the central controller 101 generates (step 1453) an aggregate hash value 1301; this value is the hash value of the aggregate of all the grid locations that the player did not pick (i.e. $h_{xy'}$). The aggregate hash value 1301 is stored in the game database 212 of the central controller (step

1454). In step 1455, the central controller 101 sends the aggregate hash value 1301 to the user computer 102, which updates the aggregate hash value field of the audit database 311.

Using hash tree techniques, the cryptoprocessor 302 of the user computer 102 takes both the information relating to the prize value corresponding to the player's selection (i.e. h_{xy}) and the aggregate hash value 1301 to calculate a hash value for the entire grid (step 1456). In step 1457, the user computer 102 uses hash tree techniques to compare this hash value for the entire grid to the hash value 1101 stored in the audit database 311. If the two values match, the integrity of the game is confirmed.

At this point, the player does not know the location of any winning locations on the grid, and therefore cannot help any other player to win. The winning grid locations are not revealed until all players have made all of their selections.

When all grid locations have been selected by all the players, the central controller 101 sends the winning grid locations to the user computer 102 (step 1458). The user computer stores the winning grid locations in the audit database 311 (step 1481). At the end of a billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1482). If money is due the customer, the central controller 101 initiates a payment to the customer according to the customer's preferred payment method 709 (step 1483).

Fourth Embodiment (Central Controller Encryption)

In the fourth embodiment of the invention, the audit database 311 in the user computer 102 has a structure as shown in Figure 15A. As in the previous embodiments, each record in the audit database corresponds to one game. A record includes the game identification number 901, selected grid location or locations 902, and the game denomination 713. In this embodiment, the record also includes a random key 1510, and encrypted and decrypted versions (1520 and 1530 respectively) of the winning grid locations.

The structure of the game database 212 in this embodiment is shown in Figure 15B. Each entry in the game database has a game identification number 901, a customer identification number 702 and the winning grid locations 903, as in the previous embodiments. The entry also has the user-selected grid location 902, the game denomination 713 and the random key 1510.

A game conducted according to the fourth embodiment of the invention begins with the steps shown in the flowchart of Figure 8 as already described above, and continues with the steps shown in the flowchart of Figure 16.

In step 1601, the central controller 101 retrieves the winning grid locations 903 for a game from the game database 212; the cryptoprocessor 202 encrypts these locations using the random key 1510. The central controller 101 then transmits the encrypted grid locations to the user computer 102 along with the "blank" electronic game board (step 1602). The player enters his grid location selections into the user computer 102, using the input device 320 (step 1603). The user computer 102 transmits the player's grid

location selection to the central controller along with the game ID number (step 1604). In step 1605, the central controller stores the player's selections in the selected grid locations field 902 of the game database 212, and then transmits the key 1510 to the user computer 102. The central controller 101 then (step 1606) compares the user selected grid locations 902 with the winning grid locations 903.

If the player is not a winner, the central controller proceeds to generate the next game (step 1650). If the player is a winner, the central controller 101 updates the total money awarded 707 in the customer database 211 to reflect the amount the player has just won (step 1610). In addition, at the end of a billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1620). If money is due the player, the central controller 101 initiates a payment to the customer according to customer's payment method preference 709 (step 1630).

It should be noted that a key element of this embodiment is that the central controller 101 sends the winning grid locations to the user computer 102 (though encrypted and thus unreadable by the user computer) before receiving the user's grid location selection. The player is thereby assured that the game provider cannot change the winning locations based upon knowledge of his selection. On the other hand, the central controller holds the player's selection before the player is provided with the key to decrypt the winning locations. The encryption of the winning locations thus assures both parties that the game has been fairly conducted.

This embodiment is particularly applicable to games such as blackjack, in which the central controller

could randomly arrange an electronic deck of cards, encrypt them, and transmit them to the player. The player then sends card selections and play decisions to the central controller.

Fifth Embodiment (Trusted Third Party)

In the fifth embodiment of the invention, a trusted third party computer 400 is used to assure the integrity of the game. The audit database 311 in the user computer 102, the audit database 411 in the trusted third party computer 400 (both shown in Figure 17A) and the game database 212 in the central controller 212 (shown in Figure 17B) have the same structure. Each record in these databases corresponds to one game. A record includes the game identification number 901, selected grid location or locations 902, the winning grid locations 903, the game denomination 713 and the customer identification number 702.

A game conducted according to the fifth embodiment of the invention begins with the steps shown in the flowchart of Figure 8 as already described above, and continues with the steps shown in the flowcharts of Figures 18A and 18B. In step 1801, the central controller 101 transmits the game identification number 901 and the winning grid locations 903 to the trusted third party 400. The central controller 101 then sends a "blank" punchboard 500 to the user computer 102 (step 1802). The player selects a grid location 902 and enters it into the user computer 102, using the input device 320 (step 1803). The player may enter additional selections if he so desires. After the player has made all of the selections for that game, the user computer 102 transmits the player's grid selections 902 to the central controller 101 (step 1810). The central controller queries the winning grid

location field 903 of the game database 212 to determine if the player's grid selection is a winner (step 1811). If the selection is a winner (step 1812), the controller notifies the player and updates the total money awarded field 707 of the customer database 211 accordingly.

The user computer 102 then transmits the game identification number to the trusted third party 400 (step 1813). The CPU 401 of the third party computer 400 queries the game identification number field 901 of the audit database 411 and retrieves the requested game identification number (step 1814). The third party computer 400 then sends the winning grid locations corresponding to the requested game identification number to the user computer 102 (step 1815).

In step 1851, the player uses the information from the trusted third party 400 to verify that the game provided by the central controller 101 was legitimate. In this embodiment, the use of the trusted third party makes encryption of player selected grid locations and winning grid locations unnecessary.

At the end of a billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1852). If money is due the player, the central controller 101 initiates a payment to the customer according to customer's payment method preference 709 (step 1853).

Many variations of the embodiments discussed above are possible. For example, the central controller can track the amount of play engaged in by individual users for marketing purposes. In particular, special advertisements could be transmitted over the Internet targeted to high volume players. The central

controller may offer demonstration games for new users so that they learn how to play. The game may be configured as a "pulltab" game, rather than punchboard. A user may be offered discounts on subsequent game, to provide him with an incentive to play again.

Although the above embodiments have been described with reference to a remote player making payments by credit card, a number of payment methods are possible. For example, the player may maintain an account with the game provider, or make payments with digital cash. Furthermore, rather than interact remotely with the central controller, the player may make his payment to a live cashier, who then enters the amount of credit into the central controller using an input device.

In addition, although the above embodiments have been described with reference to communication over the Internet, it will be appreciated that the practice of our invention is not limited to Internet communications, but is applicable to a variety of possible modes of communication between the game provider and the player. Commercial online services such as CompuServe and America Online could implement the systems and methods of the present invention.

Each of the above-described embodiments of the virtual punchboard is generally applicable to a game in which a player predicts a random outcome. One skilled in the art will appreciate how the various aspects of the virtual punchboard may be implemented in other games of chance (roulette, bingo, slot machines, blackjack, craps, lottery, etc.).

While the present invention has been described above in terms of specific embodiments, it is to be understood that the invention is not limited to the disclosed

embodiments. On the contrary, the present invention is intended to cover various modifications and equivalent structures included within the spirit and scope of the appended claims.

We claim:

1. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

wherein player selection identifier is encrypted, said computing device transmits the winning selection identifier in an unencrypted format after receiving the encrypted player selection identifier, said computing device receives the decryption key after transmitting the winning selection identifier, said computing device decrypts the encrypted player selection identifier using the cryptoprocessor and decryption key, and afterwards performs said comparing by comparing the decrypted player selection identifier with the winning selection identifier.

2. A system according to claim 1, wherein said game of chance comprises an electronically implemented punchboard.

3. A system according to claim 1, wherein said game of chance comprises an electronically implemented roulette wheel.

4. A system according to claim 1, wherein said game of chance comprises an electronically implemented bingo game.

5. A system according to claim 1, wherein said game of chance comprises an electronically implemented slot machine.

6. A system according to claim 1, wherein said game of chance comprises an electronically implemented lottery.

7. A system according to claim 1, wherein said transmitting and receiving are performed on the Internet.

8. A system according to claim 1, wherein the memory device includes a game database containing the winning selection identifier and a prize amount associated therewith.

9. A system according to claim 1, wherein said computing device further comprises a random number generator for generating a random number for use in selecting the winning selection from the plurality of available selections.

10. A system according to claim 1, wherein the memory device includes a customer database containing a customer identifier and information regarding a credit account of a customer, and the program is further adapted to initiate a charge against the credit account in accordance with the player selection and to initiate a payment to the credit account of the prize amount in accordance with the result of said game.

11. A system according to claim 1, wherein said encryption key and said decryption key are identical.

12. A system according to claim 1, wherein the encryption key is based on a random number.

13. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

wherein the cryptoprocessor generates a first value based on the winning selection identifier, and said computing device transmits the first value with the plurality of available game selections for comparison with a second value based on the transmitted winning selection identifier, the winning selection identifier transmitted after receipt of the player selection identifier, where said comparison is used to verify that the winning selection identifier and the player selection identifier were independently generated.

14. A system according to claim 13, wherein the first value and the second value are one-way hash values.

15. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

wherein the cryptoprocessor generates a first value based on the winning selection identifier, said computing device transmits the first value with the plurality of available game selections, the cryptoprocessor generates a second value based on the available game selections other than the player selection after said computing device receives the player selection identifier, and said computing device before transmitting the winning selection identifier transmits the second value, where comparison of a third value based on the player selection and the second value with the first value verifies that the winning selection identifier and the player selection identifier were independently generated.

16. A system according to claim 15, wherein the first value, the second value and the third value are one-way hash values, and the third value is generated using a hash tree algorithm.

17. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor and a memory device connected to the processor, the memory device

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : A63F

A2

(11) International Publication Number: **WO 99/01188**

(43) International Publication Date: 14 January 1999 (14.01.99)

(21) International Application Number: PCT/US98/13909

(22) International Filing Date: 2 July 1998 (02.07.98)

(30) Priority Data:
08/888,049 3 July 1997 (03.07.97) US

(71) Applicant: WALKER ASSET MANAGEMENT LIMITED PARTNERSHIP [US/US]; 5 High Ridge Park, Stamford, CT 06905–1325 (US).

(72) Inventors: WALKER, Jay, S.; 124 Spectacle Lane, Ridgefield, CT 06877 (US). SCHNEIER, Bruce; 101 East Minnehaha Parkway, Minneapolis, MN 55419 (US). JORASCH, James, A.; Apartment 5G, 25 Forest Street, Stamford, CT 06901 (US). VAN LUCHENE, Andrew, S.; 13–2A Clarmore Drive, Norwalk, CT 06850 (US).

(74) Agent: ANDERSON, Jay, H.; Fitzpatrick, Cella, Harper & Scinto, 30 Rockefeller Plaza, New York, NY 10112–3801 (US).

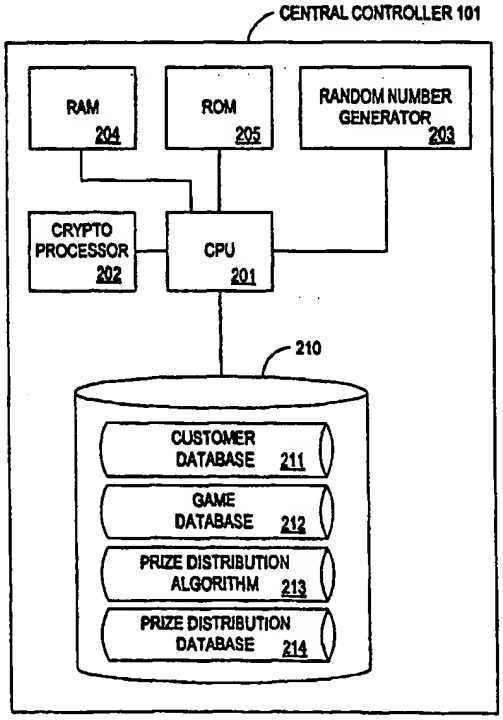
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD AND APPARATUS FOR SECURING ON–LINE VIRTUAL PUNCHBOARD TRANSACTIONS

(57) Abstract

A system is described for facilitating an Internet–based game of chance, particularly a computer–based version of a punchboard game having a grid with prizes associated with the various grid locations. The user can pay a central controller for each selection by providing a credit card number, or through other Internet transaction means. The central controller sends the user a fresh virtual punchboard (i.e. a game in which no selections have yet been made). The user selects a grid location, encrypts it, and then transmits it to the central controller. The central controller then generates prize values for the grid that it sent to the player. The user's computer stores the locations of each prize and determines whether the player's selection was a winner. If he has won, the player sends the decryption key to the central controller to decrypt his grid selection and authenticate his selection. The central controller then initiates a payment to the user.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

TITLE

METHOD AND APPARATUS FOR SECURING ON-LINE VIRTUAL PUNCHBOARD TRANSACTIONS

BACKGROUND OF THE INVENTION

This invention relates to an electronic gambling game in which a player selects from a series of possible outcomes. The player and game provider may interact in a variety of ways, including over the Internet.

A number of well-known gambling games are based on a player selecting from a series of possible outcomes, where the winning outcome is randomly generated using some physical or mechanical device furnished by the game operator. Examples of such games are roulette, slot machines, and bingo. In the classical embodiments of these games, the player sees and/or hears the outcome generated (as in bingo and roulette), or even has a hand in generating the outcome himself (as in slot machines). The player's trust in the fairness of these games (that is, his belief that the outcome is random and that his selection, if a winner, will be honored) is largely based on his personal observation. Similarly, the game operator can use various methods to prevent cheating by a player if the player is

personally present; for example, a bingo player claiming to be a winner is required to offer his card for inspection.

A well-known example of an entertainment/gambling device is the "punchboard." A punchboard consists of a board with a square grid of holes. Each hole contains a small rolled-up piece of paper. The player takes a pin and pushes through the board, pushing a selected piece of paper through the other side. This paper is then unrolled by the player to reveal whether or not he has won a prize. In a typical punchboard game, a player pays a small sum (approximately $1) to make a selection; prizes are determined by the size of the board and the fees, and may run hundreds of dollars.

Here, too, the player's confidence in the fairness of the game is largely based on his observation of the board; since he selects a piece of paper and can immediately read the message on it, he can be sure that the paper is not switched or tampered with after he selects it. In addition, by watching a number of plays he can eventually satisfy himself that there are indeed winning locations somewhere on the board. A successful electronic version of a punchboard game (a "virtual punchboard") must offer the player similar assurance that the game is not rigged, and must also prevent cheating the player.

Various forms of electronic games of chance have been available for many years. The way these games are played, however, is changing dramatically with the use of digital computers operating on electronic networks such as the Internet. Players can now connect to a remote server and wager electronically. Rather than traveling to the game (casino, bingo hall, etc.), a player can log into an electronic game and wager from

the comfort of his own home. While this remote playing has many advantages, it raises several security issues. In a typical electronic gambling game, the player enters his selection and then learns whether he has won, without observing the winning selection being generated. For example, when playing card games at a casino, a player can observe the dealer shuffle and deal the cards and thus has some confidence that the outcome was generated randomly. In an electronic casino, the shuffling process is typically digitally generated, driven by random number generators which the player cannot see. The player cannot know whether the random number generated is truly random or was selected by the casino to give it an advantage.

Furthermore, a player desiring to play an electronic game remotely (for example, communicating with a game provider on the Internet) must send his selection and receive the winning selection over a communication network. In this instance, both the player and game provider require assurance that the communications are secure and that the game is conducted fairly.

Electronic game providers have tried to increase players' confidence in the legitimacy of games by assuring players that gaming software has not been tampered with. For example, an electronic game provider may allow an independent third party to perform an audit of the software. This is a time-consuming and expensive process, however. With complex software running into the hundreds of thousands of lines of code, it is very difficult to find a few lines of code that alter the randomness of the outcomes. Also, use of an independent, third party auditor shifts the need for trust to another party, and does not guarantee the legitimacy of the game.

Some electronic lottery systems have used methods for securing communications between remote player terminals and a central controller. For example, U.S. Patent No. 4,652,998 to Koza et al. ("Video Gaming System With Pool Prize Structures") describes cryptographic methods for securing these communications. In games dependent on the use of random numbers, however, simply securing against the transmission of a fraudulent random number does not solve the problem of assuring the player that the game is fairly conducted. Nor does it solve the problem of preventing multiple players from cooperating to gain an advantage over the game provider.

U.S. Patent No. 5,326,104 to Pease et al. ("Secure Automated Electronic Casino Gaming System") describes a system whereby a number of keno playing devices, all within the same playing area, are connected to a central controller. A player can play a device by inserting a player account card into it which is registered and confirmed by the central controller. Security in this system is directed primarily to ensuring that players will not tamper with the keno terminals, and that employees will not enter false tickets into the system. Apparently it is assumed that the central controller is trusted and will not try to cheat the players.

U.S. Patent No. 5,569,082 to Kayer ("Personal Computer Lottery Game") describes a game whereby a player can purchase a game piece containing an encrypted code which determines whether the piece is a winning one. The player logs onto a central site, via a PC or a kiosk, and types in the code. The site runs a game which reveals to the player if he is a winner in "an exciting fashion." If the player is a winner, he will be given instructions by the site as to where to pick up his prize. Although the system described in this

patent provides encryption to protect the site from fraud, it offers no encryption to protect the player.

U.S. Patent No. 5,547,202 to Tsumura ("Computer Game Device") describes a system whereby a player can pay for the usage of games transmitted to his PC or to a kiosk via satellite from a central controller. The games are scrambled until payment is made. The central controller can store a game so that a player can take breaks from a game, return to it and continue play from the point in the game at which he left it. This system has neither a gambling element nor is it cryptographically enabled.

U.S. Patent No. 5,269,521 to Rossides ("Expected Value Payment Method and System For Reducing the Expected Per Unit Costs of Paying and/or Receiving a Given Amount of Commodity") describes a system where a customer exchanges encoded numbers with a product vendor. After being decoded, the two numbers are combined to determine a result. (See column 30, lines 1 to 5, as well as column 30, line 35, to column 31, line 55). The transactions described are not conducted in an online manner. Additionally, both parties must encode their numbers before exchanging them. No game results are ever exchanged in encoded form.

U.S. Patent No. 4,309,569 to Merkle ("Method of providing digital signatures") describes a system for digital signatures utilizing hash trees.

The proliferation of electronic network technology, along with the ease of user access to networks such as the Internet, has dramatically increased electronic communications and the exchange of information. Among a myriad of other uses, these networks facilitate the playing of games, including gambling activities. They

are particularly well suited for such gaming because of their ability to collapse geographic distances while linking distributed players. As discussed above, however, the electronic implementation of games, and particularly gambling activities, often results in the loss of confidence and validity otherwise imbued in players from their personal observation of traditional gaming procedures (for example, dealing cards, spinning roulette wheels, etc.).

There thus exists a need in the art for systems and procedures which can both actually and in the perception of players improve the security and operation of electronic gambling and games. Such systems and procedures would not only foster the perception of on-line gaming as legitimate, but also increase player participation in such activities. This would further increase the commercial value of what is already a substantial online business.

SUMMARY OF THE INVENTION

In accordance with the present invention there is provided a new and improved method and apparatus for facilitating computer-based games of chance on electronic networks such as the Internet. A key feature of the invention comprises the use of encoding techniques, including various encryption schemes, to validate the operation of the games and prevent cheating by either the player or the game provider. Although encryption methods are described, it should be noted that any encoding scheme which prevents the recipient of a message from deciphering its contents will suffice.

In accordance with one embodiment of the invention, a method of generating and verifying the results of a computer-based game of chance is implemented by transmitting to a player computer a plurality of available game selections, each identified by a unique selection identifier. A player selection identifier is received from the player computer, and a winning selection identifier transmitted to the player computer. The player selection identifier and the winning selection identifier are compared to determine if the player has won the game. In accordance with the invention, verification is made that the winning selection identifier and the player selection identifier were independently generated.

Game operation is preferably managed by a central controller, with players communicating with the controller through player computers connected over an electronic network. In different embodiments of the invention, verification of authenticity is provided in the central controller, the player computer, some combination of both, or with the involvement of a third party.

Games supported include all games of chance which permit a user to select from amongst a plurality of potentially winning selections. Applicable games include, but are not limited to a punchboard having punch locations, a roulette wheel having wheel numbers, a bingo game having user-selected card numbers, and a slot machine having user-selectable outcomes.

Verification is provided through a variety of techniques, including the use of encryption such as key-based encryption, and hash-based encryption. The invention further contemplates the use of a third-party

trusted agent to monitor and verify that the player and winning selections were independently generated.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram showing an overview of the system of the present invention.

Figure 2 is a block diagram of the central controller of Figure 1.

Figure 3 is a block diagram of the user computer of Figure 1.

Figure 4 is a block diagram of a trusted third party computer.

Figure 5 is a schematic representation of the punchboard game area before a game has been played.

Figure 6 is a schematic representation of the punchboard game area after a game has been played.

Figure 7A shows in tabular form the fields of the customer database of the central controller.

Figure 7B shows in tabular form the information in the prize distribution database of the central controller.

Figure 8 is a flowchart describing initiation of a game according to the preferred embodiments of the present invention.

Figure 9A shows in tabular form the information in the audit database of the user computer according to the first embodiment of the invention.

Figure 9B shows in tabular form the information in the game database of the central controller according to the first embodiment of the invention.

Figures 10A and 10B are connected flowcharts describing the flow of play between the central controller and user computer according to the first embodiment of the invention.

Figure 11A shows in tabular form the information in the audit database of the user computer according to the second embodiment of the invention.

Figure 11B shows in tabular form the information in the game database of the central controller according to the second embodiment of the invention.

Figures 12A and 12B are connected flowcharts describing the flow of play between the user computer and the central controller according to the second embodiment of the invention.

Figure 13A shows in tabular form the information in the audit database of the user computer according to the third embodiment of the invention.

Figure 13B shows in tabular form the information in the game database of the central controller according to the third embodiment of the invention.

Figures 14A, 14B and 14C are connected flowcharts describing the flow of play between the user computer and the central controller according to the third embodiment of the invention.

Figure 15A shows in tabular form the information in the audit database of the user computer according to the fourth embodiment of the invention.

Figure 15B shows in tabular form the information in the game database of the central controller according to the fourth embodiment of the invention.

Figure 16 is a flowchart describing the flow of play between the user computer and the central controller according to the fourth embodiment of the invention.

Figure 17A shows in tabular form the information in the audit database of the third party according to the fifth embodiment of the invention.

Figure 17B shows in tabular form the information in the game database of the central controller according to the fifth embodiment of the invention.

Figures 18A and 18B are connected flowcharts describing the flow of play between the user computer, the central controller, and the third party computer according to the fifth embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

An overview of the system in the preferred embodiments of the present invention is shown in Figure 1. The central controller 101, operated by the game provider, communicates with the user computer 102 (operated by the game player) over the Internet 100. Figure 2 is a schematic diagram of the structure of the central controller 101. The central controller includes a CPU 201, connected to a cryptoprocessor 202, a random number generator 203, RAM 204, ROM 205 and a data

storage device 210. The CPU 201 connects to the Internet for communication with the player's computer. The data storage device 210 includes a customer database 211, a game database 212, storage for the prize distribution algorithm 213 and a prize distribution database 214. To perform the various functions described in more detail below, the CPU 201 executes a program or programs stored in RAM 204 and/or ROM 205.

Cryptographic processor 202 supports the encoding and decoding of communications with players, as well as the authentication of players. An MC68HC16 microcontroller, commonly manufactured by Motorola Inc., may be used for cryptographic processor 202. This microcontroller utilizes a 16-bit multiply-and-accumulate instruction in the 16 MHZ configuration and requires less than one second to perform a 512-bit private key operation. Other exemplary commercially available specialized cryptographic processors include VLSI Technology's 33MHz 6868 or Semaphore Communications' 40 MHZ Roadrunner 284. Alternatively, cryptographic processor 202 may be configured as part of CPU 201.

A conventional random number generating processor may be used for random number generator 203. The HEMT integrated circuit manufactured by Fujitsu, for example, is capable of generating over one billion random numbers per second. Alternatively, random number generator 203 may be incorporated into CPU 201. Data storage device 210 may include hard disk, magnetic, or optical storage units, as well as CD-ROM drives or flash memory.

The user computer 102 is shown schematically in Figure 3. The user computer includes a CPU 301, connected to

a cryptoprocessor 302, a random number generator 303, RAM 304, ROM 305 and a data storage device 310. The CPU 301 is also connected to an input device 320 and to the Internet, for communication with the user and the central controller respectively. In addition, the CPU 301 is connected to a display device 330 for displaying a virtual punchboard to the user. The data storage device 310 includes an audit database 311. The CPU 301, cryptoprocessor 302, random number generator 303 and data storage device 310 may have the same features as CPU 201, cryptoprocessor 202, random number generator 203 and data storage device 210 discussed just above.

Figure 4 is a schematic diagram of a trusted third party computer 400, which is used in an embodiment of the invention discussed in more detail below. This computer includes a CPU 401, RAM 404, ROM 405 and data storage device 410, similar to central controller 101 and user computer 102. The data storage device includes an audit database 411. The CPU 401 is connected for communication with the user computer 102 and the central controller 101.

Figure 5 shows the appearance of a virtual punchboard display 500, displayed to a user on the display device 330, before a game is played. The game is identified by a number 510, and an empty grid 511 is shown (in this case, a 12 x 12 square). A box 512 appears where the player may enter his selected grid locations. The player's current credits 513 (how much he has paid for the present game, plus his winnings so far) may also be displayed; in the example shown, the player has no winning balance and has just made an electronic payment of $1 to play game # 6465484564.

Figure 6 shows a results display 600, similarly displayed to the user by display device 330, after the game is played. The winning locations are displayed in a table 610 and on the grid 611, with the player's selection circled on the grid and displayed in a box 612. Also displayed is the result of the game (in this case the player is told, "YOU WIN!") and the balance 613 of the player's winnings. Finally, the display includes a box 620 labeled "PLAY AGAIN?" The CPU 301 may advantageously execute interactive display software (stored in RAM 304 or ROM 305) which enables "click boxes" and the like. In that case, the player would click on the "PLAY AGAIN?" box to order a new game.

Figure 7A shows the fields of the customer database 211 maintained by the central controller 101. Each customer is identified by name 701 and is assigned an ID number 702. Each customer entry in the database also includes a credit card number 703, the customer's e-mail address 704 and postal mailing address 705, the total amount the customer has spent 706, and the customer's total winnings to that point 707. The database stores the grid selection preferences 708 for each customer (so that a player who regularly plays the same location on the grid need not enter that location in every game), and the customer's preferred method 709 of receiving his winnings.

The fields of the prize distribution database 214, maintained by the central controller 101, are shown in Figure 7B. Each prize distribution is assigned an identification number 711. Each entry in the database includes the size 712 of the grid, the denomination of the game 713 (that is, the cost to the customer for one play) and the number and amount of prizes 714 to be awarded. Generally, a larger grid has more prizes

associated therewith, and a grid with larger prizes has a larger associated denomination.

To create a new game, the central controller 101 employs a prize distribution algorithm 213 having the following steps: The central controller 101 retrieves the prize structure 714 and grid size 712 from the prize distribution database 214 by searching for the prize distribution ID number 711. The CPU 201 instructs the random number generator 203 to produce enough random numbers to cover the number of grid locations for the game. Each random number is appended to a grid location. The format might be (x,y,r), where "x" is the x-coordinate of the grid location, "y" is the y-coordinate of the grid location, and "r" is the assigned random number. The random numbers are then ranked numerically. Prizes are then appended to each grid location. The format might be (x,y,r,p), with "p" the prize value (which may be zero) assigned to the grid location (x,y). The game is then assigned an ID number. The winning grid locations for the game, and the prizes associated with those locations, are then stored in the game database 212, detailed embodiments of which are described below. Those skilled in the art will appreciate that there are many possible algorithms by which the prices may be randomly assigned. The above algorithm is merely illustrative

First Embodiment (User Computer Encryption)

In the first embodiment of the invention, the fields of the audit database 311 (stored in the user computer 102) are as shown in Figure 9A. Each record in the audit database 311 corresponds to one game played by the user, and is filled in as the game progresses (as described in detail below). A record includes an identification number 901 for the game, the grid

location or locations 902 selected by the player, the winning grid locations 903, the game denomination 713, and a random key 904 which the player uses to encrypt his grid location selections.

In this embodiment, the fields of the game database 212 (stored in the central controller 101) are as shown in Figure 9B. Each record in the game database corresponds to one game (having an ID number 901) played by one player (having an ID number 702). Each record includes the winning grid locations 903, the player's selected and encrypted grid location 910, the corresponding decrypted grid location 920, and the player key 904.

A game conducted according to the first embodiment of the invention begins with the steps shown in the flowchart of Figure 8. Initially, the player (using his computer 102) logs on to the central controller 101 via the Internet 100 (step 801). If the player does not yet have an account (that is, an entry in the customer database 211), an account is opened at this time; the player provides the necessary information (step 804), and the central controller 101 assigns him an ID number and stores the new record in the customer database 211 (step 805). If the player already has an account, he enters his customer ID number 702 (step 810).

The player then selects the amount of money he wishes to play--that is, the denomination of the game; for example, $1, $3, or $5 (step 820). The user computer 102 updates the denomination field 713 in the audit database 311 (step 830). The central controller 101 debits the credit card account of the player for the amount of money played (step 840). The central controller 101 retrieves a new game grid from the prize distribution database 214 (step 850). Using the prize

distribution algorithm 213 described above, the central controller 101 generates the winning grid locations 903, assigns the game identification number 901 and stores the game in the game database 212 (step 860).

In this embodiment, the game continues with the steps shown in the flowcharts of Figures 10A and 10B. In step 1001 of Figure 10A, a "blank" punchboard 500 including the game identification number 510 is made available to the player. The player selects a grid location 902 and enters it into the user computer 102 using input device 320 (step 1002). The cryptographic processor 302 of the user computer 102 generates a player key 904, preferably based on a random number generated by random number generator 303 (step 1003). The cryptographic processor 302 encrypts the grid location selection 902 with the player key (step 1004). The user computer 102 stores the game identification number, player key, and grid location selection in the audit database 311 (step 1005).

In step 1006, the encrypted grid location and game identification number are transmitted to the central controller 101. The central controller then retrieves the record in the game database 212 corresponding to the game identification number received from the user computer 102 (step 1007). The central controller 101 stores the encrypted grid location 910 in the game database 212 (step 1008).

At this point, the central controller 101 has the player's grid location selection, but only in an encrypted form. The central controller 101 then transmits the winning grid locations 903 to the user computer 102 (step 1010 of Figure 10B).

If the player has not won, he may proceed to select a new game (step 1061). If the player has won, the user computer 102 transmits the player key 904 and game identification number to the central controller 101 (step 1051). The central controller decrypts the encrypted grid location 910, and stores the decryption result 920 (the player's selected, winning grid location) and player key 904 in the game database 212 (step 1052).

The amount of money won by the player is retrieved from winning grid location field 903 of the game database 212 (step 1053). The central controller 101 then sends the game result message 600 to the user computer 102, indicating that the player has won (step 1054). The central controller then proceeds to generate the next game (step 1055).

At the end of the billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1056). If money is due the customer, the central controller 101 initiates a payment to the customer according to the customer's preferred payment method 709 (step 1057).

It should be noted that a key element of this embodiment is that the user sends his grid location selection in encrypted form (thus unreadable by the central controller 101) to the central controller before receiving the winning grid locations. The player is thereby assured that the game provider cannot change the winning locations based upon knowledge of his selection. On the other hand, the central controller holds the player's encrypted selection before the player is given the winning locations, and the player must provide the key to decrypt his selection before the central controller awards him a

prize. The encryption of the player's selection thus assures both parties that the game has been fairly conducted, and that the two numbers were independently generated.

A transmission between the central controller and the player may include a digital signature to provide further assurance of the authenticity of the transmission, and to prevent repudiation by the sender. The uses and advantages of digital signatures are discussed generally in Schneier, "Applied Cryptography" (2d ed. 1996), chapter 2.

The above embodiment is also applicable to a game such as roulette. Instead of encoding his grid location selection, the player encrypts his number selection (representing any of the 38 wheel slots). The central controller then transmits the result of the wheel spin to the player.

The game of bingo could be simulated as follows. The player selects a board and then encrypts his selection before sending it to the central controller. The central controller then sends out each bingo number until one of the players claims a win. The winning player sends his key to the central controller so that his selection can be verified.

To simulate a slot machine, the player simply selects one of the possible reel combinations of the slot machine. In a slot machine with three reels and 20 stops per reel, there are 8,000 (20 X 20 X 20) possible outcomes, so the player could select one of these at random, encrypting the selection and sending it to the central controller. The central controller then distributes the prizes among the possible outcomes and

sends the complete set of outcomes to the player so that he can determine whether or not he has won.

Second Embodiment (One-Way Hash)

In the second embodiment of the invention, the audit database 311 in the user computer 102 has a structure as shown in Figure 11A. As in the first embodiment, each record in the audit database corresponds to one game. A record includes the game identification number 901, selected grid location or locations 902, winning grid locations 903 and the game denomination 713, similar to the record shown in Figure 9A. In this embodiment, the record also includes the hash value 1101 of the winning grid locations 903.

The structure of the game database 212 in this embodiment is shown in Figure 11B. Each entry in the game database has a game identification number 901, a customer identification number 702 and the winning grid locations 903, as in the first embodiment. The entry also has the user-selected grid location 902 and the hash value 1101 of the winning grid locations 903.

A game conducted according to the second embodiment of the invention begins with the steps shown in the flowchart of Figure 8 as already described above, and continues with the steps shown in the flowcharts of Figures 12A and 12B. In step 1201 of Figure 12A, the cryptoprocessor 202 of the central controller 101 retrieves the winning grid locations 903 of the game from the game database 212, and uses a one-way hash function to hash the winning grid locations 903, thereby generating the hash value 1101. The hash value 1101 represents a one-way transformation of the winning grid locations 903.

An important feature of the one-way hash function is that it is computationally simple (given the hash function) to generate the hash value, but computationally unfeasible to recreate the winning grid locations from the hash value alone. The hash value 1101 thus serves as a unique identifier for the winning grid locations 903, without the winning grid locations themselves being revealed. Further details on one-way hash functions are given in Schneier, "Applied Cryptography" (2d ed. 1996), chapter 18.

The central controller 101 distributes the hash value 1101 to the user computer 102, along with a "blank" punchboard 500 with game identification number 510 (step 1202). The user computer 102 stores the hash value and game ID number in the audit database 311 (step 1203). In step 1204, the player selects a grid location and enters it into the user computer 102; the player may make additional grid location selections. Once the player has made all of his selections, the user computer 102 stores the game identification number 901, the selected grid locations 902 and the hash value 1101 in the audit database 311 (step 1211). The user computer 102 transmits the selected grid locations 902 to the central controller 101 along with the game ID number (step 1212). It should be noted that at this point the central controller 101 has the player's selections, but has already provided the player with a representation of the winning grid locations in the form of the hash value 1101. In step 1213, the central controller 101 determines whether the player has chosen a winning grid location by comparing the selected locations 902 with the winning grid locations 903 for that game.

Referring now to Figure 12B, the central controller 101 sends the winning grid locations 903 to the user

computer 102 (step 1251). In step 1252, the user computer 102 verifies the fairness of the game. Specifically, the cryptographic processor 302 of the user computer 102 applies the one-way hash function to the received winning grid locations to verify that the hash value 1101 given to him before sending his selection is equal to the new hash value calculated by applying the one-way hash function to the winning grid locations.

If the player has not won, the central controller 101 proceeds to generate the next game (step 1270). If the player has won, the central controller 101 updates the total money awarded 707 in the customer database 211 to reflect the amount the player has just won (step 1260), and then generates the next game. In addition, at the end of a billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1280). If money is due the player, the central controller 101 initiates a payment to the customer according to customer's payment method preference 709 (step 1281).

It should be noted that in this embodiment the punchboard cannot be reused; it must be replaced with a fresh punchboard after each player selection. If the punchboard were not replaced, the player could continue to select grid locations after receiving the winning grid locations 903 (see step 1251). The player could, however, make more than one selection during a game session (see step 1204), as long as each selection was received by the central controller 101 before the winning locations were transmitted to the player.

With minor modifications, this embodiment of the invention can accommodate any number of players. By delaying the transmission of the winning grid locations

until after all grid location selections have been received, any number of players can be accommodated with one punchboard. Alternatively, games could be conducted at great speed, preventing players from cheating by sharing winning locations. For example, two players might make selections on the same punchboard nearly simultaneously. The first player sends his grid location selection and then receives the winning grid locations. A fraction of a second later the second player sends his grid location selection. If the first player can communicate with the second player he can inform the second player of the winning grid locations, ensuring a win for the second player. If the time difference between the two plays is small enough, however, the first player will not have enough time to communicate the winning locations.

Third Embodiment (Hash Tree)

The third embodiment of the invention uses hash trees to accommodate multiple players in a single punchboard game. Details of hash tree techniques are well known in the art and for reference purposes are discussed in Merkle (U.S. Patent No. 4,309,569).

In this embodiment, each grid location is represented by $(x,y,p,h_{xy'})$, where x and y are the coordinates, p is the prize associated with that location, h_{xy} is the hash value of that location, and $h_{xy'}$ is an aggregate hash value for all the other locations. Furthermore, a hash value, h, is calculated for the entire grid (including all locations) using hash function H. This function has the property $H(h) = H(h_{xy},h_{xy'})$ That is, the hash value for the entire grid is equal to the hash value of one location combined with the locations's $h_{xy'}$ value. For additional security, a random number may be

attached to each grid location to provide greater variation in the resulting hash values.

In this embodiment of the invention, the audit database 311 in the user computer 102 has a structure as shown in Figure 13A. As in the previous embodiments, each record in the audit database corresponds to one game. A record includes the game identification number 901, selected grid location or locations 902, winning grid locations 903 and the game denomination 713, similar to the records shown in Figures 9A and 11A. In this embodiment, the record also includes the hash value 1101 for all grid locations (both winning and losing), and an aggregate hash value 1301, representing the hash value of the aggregate of all the grid locations not selected by the player (i.e. the h_{xy} values of all the grid locations selected by the player).

The structure of the game database 212 in this embodiment is shown in Figure 13B. Each entry in the game database has a game identification number 901, a customer identification number 702 and the winning grid locations 903, as in the previous embodiments. The entry also has the user-selected grid location 902, the denomination 713 of the game, the hash value 1101 for all grid locations, and the aggregate hash value 1301.

A game conducted according to the third embodiment of the invention begins with the steps shown in the flowchart of Figure 8 as already described above, and continues with the steps shown in the flowcharts of Figures 14A, 14B and 14C.

In step 1401, the cryptoprocessor 202 of the central controller 101 retrieves the value of all grid locations of the game from the game database 212, and uses one-way hash function H stored in the memory (RAM

204 or ROM 205) of the central controller to hash these grid locations, thereby generating h, the hash value 1101 (i.e. the hash value of all grid locations). The central controller 101 then (step 1402) distributes the hash value 1101 to the user computer 102, along with a "blank" punchboard 500 including the game identification number 510. The user computer 102 stores the hash value 1101 in the audit database 311 (step 1403). The player selects a grid location 902 and enters it into the user computer 102, using the input device 320 (step 1404). The player may enter additional selections if he so desires. After the player has made all of the selections for that game, a new record is entered in the audit database 311 of the user computer 102, reflecting the ID number for the game and the player's selected grid locations (step 1410). The user computer 102 then transmits the player's grid selections 902 and game ID number to the central controller 101 along with the game ID number (step 1411).

The central controller then (step 1451) queries the game database 212 to obtain the winning grid locations 903, to determine whether or not the player's grid selections correspond to the winning grid locations. The central controller 101 sends a message to the user computer 102 relating whether the player has won (step 1452).

The integrity of the game is verified in steps 1453 through 1457. Using the hash tree algorithm, the cryptoprocessor 202 of the central controller 101 generates (step 1453) an aggregate hash value 1301; this value is the hash value of the aggregate of all the grid locations that the player did not pick (i.e. $h_{xy'}$). The aggregate hash value 1301 is stored in the game database 212 of the central controller (step

1454). In step 1455, the central controller 101 sends the aggregate hash value 1301 to the user computer 102, which updates the aggregate hash value field of the audit database 311.

Using hash tree techniques, the cryptoprocessor 302 of the user computer 102 takes both the information relating to the prize value corresponding to the player's selection (i.e. h_{xy}) and the aggregate hash value 1301 to calculate a hash value for the entire grid (step 1456). In step 1457, the user computer 102 uses hash tree techniques to compare this hash value for the entire grid to the hash value 1101 stored in the audit database 311. If the two values match, the integrity of the game is confirmed.

At this point, the player does not know the location of any winning locations on the grid, and therefore cannot help any other player to win. The winning grid locations are not revealed until all players have made all of their selections.

When all grid locations have been selected by all the players, the central controller 101 sends the winning grid locations to the user computer 102 (step 1458). The user computer stores the winning grid locations in the audit database 311 (step 1481). At the end of a billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1482). If money is due the customer, the central controller 101 initiates a payment to the customer according to the customer's preferred payment method 709 (step 1483).

Fourth Embodiment (Central Controller Encryption)

In the fourth embodiment of the invention, the audit database 311 in the user computer 102 has a structure as shown in Figure 15A. As in the previous embodiments, each record in the audit database corresponds to one game. A record includes the game identification number 901, selected grid location or locations 902, and the game denomination 713. In this embodiment, the record also includes a random key 1510, and encrypted and decrypted versions (1520 and 1530 respectively) of the winning grid locations.

The structure of the game database 212 in this embodiment is shown in Figure 15B. Each entry in the game database has a game identification number 901, a customer identification number 702 and the winning grid locations 903, as in the previous embodiments. The entry also has the user-selected grid location 902, the game denomination 713 and the random key 1510.

A game conducted according to the fourth embodiment of the invention begins with the steps shown in the flowchart of Figure 8 as already described above, and continues with the steps shown in the flowchart of Figure 16.

In step 1601, the central controller 101 retrieves the winning grid locations 903 for a game from the game database 212; the cryptoprocessor 202 encrypts these locations using the random key 1510. The central controller 101 then transmits the encrypted grid locations to the user computer 102 along with the "blank" electronic game board (step 1602). The player enters his grid location selections into the user computer 102, using the input device 320 (step 1603). The user computer 102 transmits the player's grid

location selection to the central controller along with the game ID number (step 1604). In step 1605, the central controller stores the player's selections in the selected grid locations field 902 of the game database 212, and then transmits the key 1510 to the user computer 102. The central controller 101 then (step 1606) compares the user selected grid locations 902 with the winning grid locations 903.

If the player is not a winner, the central controller proceeds to generate the next game (step 1650). If the player is a winner, the central controller 101 updates the total money awarded 707 in the customer database 211 to reflect the amount the player has just won (step 1610). In addition, at the end of a billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1620). If money is due the player, the central controller 101 initiates a payment to the customer according to customer's payment method preference 709 (step 1630).

It should be noted that a key element of this embodiment is that the central controller 101 sends the winning grid locations to the user computer 102 (though encrypted and thus unreadable by the user computer) before receiving the user's grid location selection. The player is thereby assured that the game provider cannot change the winning locations based upon knowledge of his selection. On the other hand, the central controller holds the player's selection before the player is provided with the key to decrypt the winning locations. The encryption of the winning locations thus assures both parties that the game has been fairly conducted.

This embodiment is particularly applicable to games such as blackjack, in which the central controller

could randomly arrange an electronic deck of cards, encrypt them, and transmit them to the player. The player then sends card selections and play decisions to the central controller.

Fifth Embodiment (Trusted Third Party)

In the fifth embodiment of the invention, a trusted third party computer 400 is used to assure the integrity of the game. The audit database 311 in the user computer 102, the audit database 411 in the trusted third party computer 400 (both shown in Figure 17A) and the game database 212 in the central controller 212 (shown in Figure 17B) have the same structure. Each record in these databases corresponds to one game. A record includes the game identification number 901, selected grid location or locations 902, the winning grid locations 903, the game denomination 713 and the customer identification number 702.

A game conducted according to the fifth embodiment of the invention begins with the steps shown in the flowchart of Figure 8 as already described above, and continues with the steps shown in the flowcharts of Figures 18A and 18B. In step 1801, the central controller 101 transmits the game identification number 901 and the winning grid locations 903 to the trusted third party 400. The central controller 101 then sends a "blank" punchboard 500 to the user computer 102 (step 1802). The player selects a grid location 902 and enters it into the user computer 102, using the input device 320 (step 1803). The player may enter additional selections if he so desires. After the player has made all of the selections for that game, the user computer 102 transmits the player's grid selections 902 to the central controller 101 (step 1810). The central controller queries the winning grid

location field 903 of the game database 212 to determine if the player's grid selection is a winner (step 1811). If the selection is a winner (step 1812), the controller notifies the player and updates the total money awarded field 707 of the customer database 211 accordingly.

The user computer 102 then transmits the game identification number to the trusted third party 400 (step 1813). The CPU 401 of the third party computer 400 queries the game identification number field 901 of the audit database 411 and retrieves the requested game identification number (step 1814). The third party computer 400 then sends the winning grid locations corresponding to the requested game identification number to the user computer 102 (step 1815).

In step 1851, the player uses the information from the trusted third party 400 to verify that the game provided by the central controller 101 was legitimate. In this embodiment, the use of the trusted third party makes encryption of player selected grid locations and winning grid locations unnecessary.

At the end of a billing cycle, the central controller 101 queries the customer database 211 to see if the customer is owed money (step 1852). If money is due the player, the central controller 101 initiates a payment to the customer according to customer's payment method preference 709 (step 1853).

Many variations of the embodiments discussed above are possible. For example, the central controller can track the amount of play engaged in by individual users for marketing purposes. In particular, special advertisements could be transmitted over the Internet targeted to high volume players. The central

controller may offer demonstration games for new users so that they learn how to play. The game may be configured as a "pulltab" game, rather than punchboard. A user may be offered discounts on subsequent game, to provide him with an incentive to play again.

Although the above embodiments have been described with reference to a remote player making payments by credit card, a number of payment methods are possible. For example, the player may maintain an account with the game provider, or make payments with digital cash. Furthermore, rather than interact remotely with the central controller, the player may make his payment to a live cashier, who then enters the amount of credit into the central controller using an input device.

In addition, although the above embodiments have been described with reference to communication over the Internet, it will be appreciated that the practice of our invention is not limited to Internet communications, but is applicable to a variety of possible modes of communication between the game provider and the player. Commercial online services such as CompuServe and America Online could implement the systems and methods of the present invention.

Each of the above-described embodiments of the virtual punchboard is generally applicable to a game in which a player predicts a random outcome. One skilled in the art will appreciate how the various aspects of the virtual punchboard may be implemented in other games of chance (roulette, bingo, slot machines, blackjack, craps, lottery, etc.).

While the present invention has been described above in terms of specific embodiments, it is to be understood that the invention is not limited to the disclosed

embodiments. On the contrary, the present invention is intended to cover various modifications and equivalent structures included within the spirit and scope of the appended claims.

We claim:

1. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

wherein player selection identifier is encrypted, said computing device transmits the winning selection identifier in an unencrypted format after receiving the encrypted player selection identifier, said computing device receives the decryption key after transmitting the winning selection identifier, said computing device decrypts the encrypted player selection identifier using the cryptoprocessor and decryption key, and afterwards performs said comparing by comparing the decrypted player selection identifier with the winning selection identifier.

2. A system according to claim 1, wherein said game of chance comprises an electronically implemented punchboard.

3. A system according to claim 1, wherein said game of chance comprises an electronically implemented roulette wheel.

4. A system according to claim 1, wherein said game of chance comprises an electronically implemented bingo game.

5. A system according to claim 1, wherein said game of chance comprises an electronically implemented slot machine.

6. A system according to claim 1, wherein said game of chance comprises an electronically implemented lottery.

7. A system according to claim 1, wherein said transmitting and receiving are performed on the Internet.

8. A system according to claim 1, wherein the memory device includes a game database containing the winning selection identifier and a prize amount associated therewith.

9. A system according to claim 1, wherein said computing device further comprises a random number generator for generating a random number for use in selecting the winning selection from the plurality of available selections.

10. A system according to claim 1, wherein the memory device includes a customer database containing a customer identifier and information regarding a credit account of a customer, and the program is further adapted to initiate a charge against the credit account in accordance with the player selection and to initiate a payment to the credit account of the prize amount in accordance with the result of said game.

11. A system according to claim 1, wherein said encryption key and said decryption key are identical.

12. A system according to claim 1, wherein the encryption key is based on a random number.

13. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

wherein the cryptoprocessor generates a first value based on the winning selection identifier, and said computing device transmits the first value with the plurality of available game selections for comparison with a second value based on the transmitted winning selection identifier, the winning selection identifier transmitted after receipt of the player selection identifier, where said comparison is used to verify that the winning selection identifier and the player selection identifier were independently generated.

14. A system according to claim 13, wherein the first value and the second value are one-way hash values.

15. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

wherein the cryptoprocessor generates a first value based on the winning selection identifier, said computing device transmits the first value with the plurality of available game selections, the cryptoprocessor generates a second value based on the available game selections other than the player selection after said computing device receives the player selection identifier, and said computing device before transmitting the winning selection identifier transmits the second value, where comparison of a third value based on the player selection and the second value with the first value verifies that the winning selection identifier and the player selection identifier were independently generated.

16. A system according to claim 15, wherein the first value, the second value and the third value are one-way hash values, and the third value is generated using a hash tree algorithm.

17. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor and a memory device connected to the processor, the memory device

containing a program, adapted to be executed by the processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

wherein the cryptoprocessor encrypts the winning selection identifier using a selected encryption key, said computing device transmits the encrypted winning selection identifier before receiving the player selection identifier, and said computing device transmits the selected encryption key after receiving the player selection.

18. A system according to claim 17, wherein said computing device transmits a digital signed encrypted winning selection identifier.

19. A system according to claim 17, wherein the encryption key is based on a random number.

20. A system for facilitating a computer-based game of chance, comprising:

a first computing device including a first processor and a first memory device connected to the first processor; and

a second computing device, including a second processor and a second memory device connected to the second processor,

the first memory device containing a first program, adapted to be executed by the first processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by

a player selection identifier, transmitting a winning selection identifier,and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance,

and

the second memory device containing a second program, adapted to be executed by the second processor, for receiving the winning selection identifier from said first computing device and transmitting the winning selection identifier after said first computing device receives the player selection identified by the player selection identifier.

21. A system for facilitating a computer-based game of chance, comprising:

a first computing device including a first processor, a first cryptoprocessor connected to the first processor and a first memory device connected to the first processor, the first memory device containing a first program, adapted to be executed by the first processor, for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier,and comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance; and

a second computing device, including a second processor, a second cryptoprocessor connected to the second processor and a second memory device connected to the second processor, the second memory device containing a second program, adapted to be executed by the second processor, for receiving the plurality of available game selections from said first computing

device, transmitting to the first computing device the player selection identified by the player selection identifier, and receiving the winning selection identifier from the first computing device.

22. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

transmitting to a player computer a plurality of available game selections each identified by a unique selection identifier;

receiving from said player computer a player selection identified by a player selection identifier;

transmitting to said player computer a winning selection identifier;

comparing said player selection identifier with said winning selection identifier to determine if said player has won said game of chance; and

verifying that said winning selection identifier and said player selection identifier were independently generated.

23. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

a first transmitting step of transmitting to a player computer a plurality of available game selections each identified by a unique selection identifier;

a first receiving step of receiving from said player computer an encrypted player selection using a selected encryption key to generate an encrypted player selection identifier;

transmitting, after said first receiving step, to said player computer a winning selection identifier in an unencrypted format;

comparing said player selection identifier with said winning selection identifier to determine if said player has won said game of chance;

a second receiving step of receiving from said player computer said selected encryption method;

decrypting said encrypted selected selection identifier using said selected encryption key; and

comparing the decrypted player selection identifier with said winning selection identifier to verify that said player has won said game of chance.

24. A method according to claim 22, wherein said game of chance comprises an electronically implemented punchboard.

25. A method according to claim 22, wherein said game of chance comprises an electronically implemented roulette wheel.

26. A method according to claim 22, wherein said game of chance comprises an electronically implemented bingo game.

27. A method according to claim 22, wherein said game of chance comprises an electronically implemented slot machine.

28. A method according to claim 22, wherein said game of chance comprises an electronically implemented lottery.

29. A method according to claim 22, wherein said transmitting and receiving are performed on an electronic network.

30. A method according to claim 29, wherein said electronic network includes a commercial online service provider

31. A method according to claim 22, wherein the selected encryption key is based on a random number.

32. A method for generating and verifying results of a computer-based game of chance, the method comprising the steps of:

generating a winning selection identifier and a first value based thereon;

transmitting to a player computer the first value and a plurality of available game selections each identified by a unique selection identifier;

receiving from said player computer a player selection identified by a player selection identifier;

transmitting the winning selection identifier to said player computer after receiving said player selection identifier;

comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance; and

said first value for comparison with a second value based on said transmitted winning selection identifier to verify that the winning selection identifier and the player selection identifier were independently generated.

33. A method according to claim 32, wherein the first value and the second value are one-way hash values.

34. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

generating a winning selection identifier and a first value based thereon;

transmitting to a player computer the first value and a plurality of available game selections each identified by a unique selection identifier;

receiving from said player computer a player selection identified by a player selection identifier;

generating, after said receiving step, a second value based on the available game selections other than the player selection;

transmitting the second value to said player computer;

transmitting a winning selection identifier, after said step of transmitting the second value;

generating a third value based on the player selection and the second value;

comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance; and

comparing the third value with the first value to verify that the winning selection identifier and the player selection identifier were independently generated.

35. A method according to claim 34, wherein the first value, the second value and the third value are one-way hash values, and the third value is generated using a hash tree algorithm.

36. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

transmitting to a player computer a plurality of available game selections each identified by a unique selection identifier;

encrypting a winning selection identifier using a selected encryption key;

transmitting the encrypted winning selection identifier to said player computer;

receiving, after said step of transmitting the encrypted winning selection identifier, a player selection identified by a player selection identifier;

transmitting, after said step of receiving the player selection, the selected encryption key to said player computer; and

comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance.

37. A method according to claim 36, wherein said step of transmitting the encrypted selection identifier includes digitally signing said encrypted selection identifier.

38. A method according to claim 36, wherein the encryption key is based on a random number.

39. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

transmitting to a player computer a plurality of available game selections each identified by a unique selection identifier;

transmitting to a third-party computer a winning selection identifier;

receiving, after said step of transmitting the winning selection identifier, from said player computer a player selection identified by a player selection identifier;

transmitting, after said receiving step, the winning selection identifier to said player computer; and

comparing said player selection identifier with said winning selection identifier to determine a result of said game of chance.

40. A device for facilitating a game of chance, comprising:

a first computing device including a first processor, a first cryptoprocessor connected to the first processor and a first memory device connected to the first processor and containing a first program and a database containing information regarding a player of said game and a distribution of prizes for said game; and

a second computing device including a second processor, a second cryptoprocessor connected to the second processor, a second memory device connected to the second processor and containing a second program and a database containing information regarding game selections made by the player during said game, an input device connected to the second processor for inputting the game selections, and a display device connected to the second processor for displaying a result of said game,

the first program being adapted to be executed by the first processor for transmitting a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier, transmitting a winning selection identifier, and comparing said player selection identifier with said winning selection identifier to determine the result of said game, and

the second program being adapted to be executed by the second processor for receiving the plurality of available game selections from said first computing device, transmitting to the first computing device the player selection identified by the player selection identifier, and receiving the winning selection identifier from the first computing device.

41. A device according to claim 40, wherein said first computing device and said second computing device each further comprise means for communicating on the Internet.

42. A device according to claim 40, wherein said first computing device further comprises a first random number generator for generating a random number used by the first cryptoprocessor, and said second computing device further comprises a second random number generator for generating a random number used by the second cryptoprocessor.

43. A computer readable medium in which is stored computer readable code to be executed by a computer, said computer readable code performing a method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

transmitting to a player computer a plurality of available game selections each identified by a unique selection identifier;

receiving from said player computer a player selection identified by a player selection identifier;

transmitting to said player computer a winning selection identifier;

comparing said player selection identifier with said winning selection identifier to determine if said player has won said game of chance; and

verifying that said winning selection identifier and said player selection identifier were independently generated.

44. A computer readable medium according to claim 43, wherein communication between said computer and said player computer is performed on the Internet.

45. A method of participating in a computer-based game of chance, comprising the steps of:

receiving a plurality of available game selections each identified by a unique selection identifier;

transmitting a player selection identified by a player selection identifier;

receiving a winning selection identifier identifying a winning selection; and

verifying that the winning selection identifier and the player selection identifier were independently generated.

46. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor, an input device connected to the processor, a display device connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for receiving a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier input from the input device, encrypting the player selection identifier using the cryptoprocessor according to an encryption key, transmitting the encrypted player selection identifier, receiving a winning selection identifier, transmitting the encryption key, comparing the player selection identifier with the winning selection identifier and displaying on the display device a result of said game of chance,

wherein said computing device receives the winning selection identifier in an unencrypted format after transmitting the encrypted player selection identifier, transmits the encryption key after receiving the

winning selection identifier, and performs said comparing to verify the result of said game of chance.

47. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor, an input device connected to the processor, a display device connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for receiving a plurality of available game selections each identified by a unique selection identifier and a first value based on a winning selection identifier, storing the first value in the memory device, receiving a player selection identified by a player selection identifier input from the input device, transmitting the player selection identifier, receiving the winning selection identifier, generating a second value using the cryptoprocessor based on the received winning selection identifier, comparing said first value with said second value and displaying on the display device a result of said game of chance,

wherein the result of said game of chance is based on a comparison of the player selection identifier with the winning selection identifier, and said computing device compares said first value with said second value to verify that the winning selection identifier and the player selection identifier were independently generated.

48. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor, an input device connected to the processor, a display device connected to the processor and a memory device

connected to the processor, the memory device containing a program, adapted to be executed by the processor, for receiving a plurality of available game selections each identified by a unique selection identifier and a first value based on a winning selection identifier, storing the first value in the memory device, receiving a player selection identified by a player selection identifier input from the input device, transmitting the player selection identifier, receiving a second value based on the available game selections other than the player selection, generating a third value based on the player selection and the second value using the cryptoprocessor, comparing the third value with the first value, receiving the winning selection identifier, and displaying on the display device a result of said game of chance,

wherein the result of said game of chance is based on a comparison of the player selection identifier with the winning selection identifier, said computing device receives the second value before receiving the winning selection identifier, and said computing device compares the third value with the first value to verify that the winning selection identifier and the player selection identifier were independently generated.

49. A system for facilitating a computer-based game of chance, comprising:

a computing device including a processor, a cryptoprocessor connected to the processor, an input device connected to the processor, a display device connected to the processor and a memory device connected to the processor, the memory device containing a program, adapted to be executed by the processor, for receiving a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier input from the input

device, receiving a winning selection identifier in an encrypted format, transmitting the player selection identifier, receiving an encryption key, decrypting the encrypted winning selection identifier using the cryptoprocessor and the encryption key, and displaying on the display device a result of said game of chance,

wherein said computing device receives the encrypted winning selection identifier before transmitting the player selection identifier and receives the encryption key after transmitting the player selection identifier, and the result of said game of chance is based on a comparison of the player selection identifier with the winning selection identifier.

50. A system for facilitating a computer-based game of chance, comprising:

a first computing device including a first processor, an input device connected to the first processor, a display device connected to the first processor and a first memory device connected to the first processor; and

a second computing device, including a second processor and a second memory device connected to the second processor,

the first memory device containing a first program, adapted to be executed by the first processor, for receiving a plurality of available game selections each identified by a unique selection identifier, receiving a player selection identified by a player selection identifier input from the input device, transmitting the player selection identifier, receiving a winning selection identifier from said second computing device, and displaying on the display device a result of said game of chance, and

the second memory device containing a second program, adapted to be executed by the second

processor, for transmitting the winning selection identifier to said first computing device after said first computing device transmits the player selection identifier,

wherein the result of said game of chance is based on a comparison of the player selection identifier with the winning selection identifier.

51. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

receiving a plurality of available game selections each identified by a unique selection identifier;

inputting a player selection identified by a player selection identifier;

encrypting the player selection identifier using an encryption key;

transmitting the encrypted player selection identifier;

receiving a winning selection identifier;

comparing the player selection identifier with the winning selection identifier to determine if said player has won said game of chance; and

transmitting the encryption key,

wherein the winning selection identifier is received in an unencrypted format after the encrypted player selection identifier is transmitted, the encryption key is transmitted after the winning selection identifier is received, and a comparison of the player selection identifier with the winning selection identifier verifies that said player has won said game of chance.

52. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

receiving a plurality of available game selections each identified by a unique selection identifier and a first value based on a winning selection identifier;

inputting a player selection identified by a player selection identifier;

transmitting the player selection identifier;

receiving the winning selection identifier;

generating a second value based on the received winning selection identifier; and

comparing said first value with said second value to verify that the winning selection identifier and the player selection identifier were independently generated.

53. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

receiving a plurality of available game selections each identified by a unique selection identifier and a first value based on a winning selection identifier;

inputting a player selection identified by a player selection identifier;

transmitting the player selection identifier;

receiving a second value based on the available game selections other than the player selection;

generating a third value based on the player selection and the second value;

comparing the third value with the first value; and

receiving the winning selection identifier;

wherein the second value is received before the winning selection identifier is received, and said step of comparing the third value with the first value verifies that the winning selection identifier and the player selection identifier were independently generated.

54. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

receiving a plurality of available game selections each identified by a unique selection identifier;

inputting a player selection identified by a player selection identifier;

receiving a winning selection identifier in an encrypted format;

transmitting the player selection identifier;

receiving an encryption key; and

decrypting the encrypted winning selection identifier in accordance with the encryption key,

wherein the encrypted winning selection identifier is received before the player selection identifier is transmitted, the encryption key is received after the player selection identifier is transmitted, and a comparison of the player selection identifier with the winning selection identifier decrypted according to the encryption key verifies that said player has won said game of chance.

55. A method of generating and verifying results of a computer-based game of chance, the method comprising the steps of:

receiving from a game server computer a plurality of available game selections each identified by a unique selection identifier;

inputting a player selection identified by a player selection identifier;

transmitting the player selection identifier to the game server computer; and

receiving from a third-party computer a winning selection identifier,

wherein the winning selection identifier is received from the third-party computer after said step of transmitting the player selection identifier.

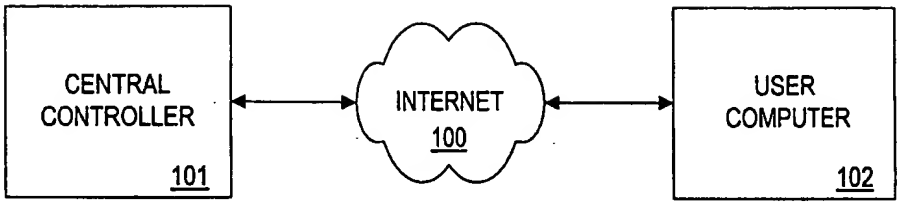

CENTRAL CONTROLLER
101
INTERNET
100
USER COMPUTER
102

FIG. 1

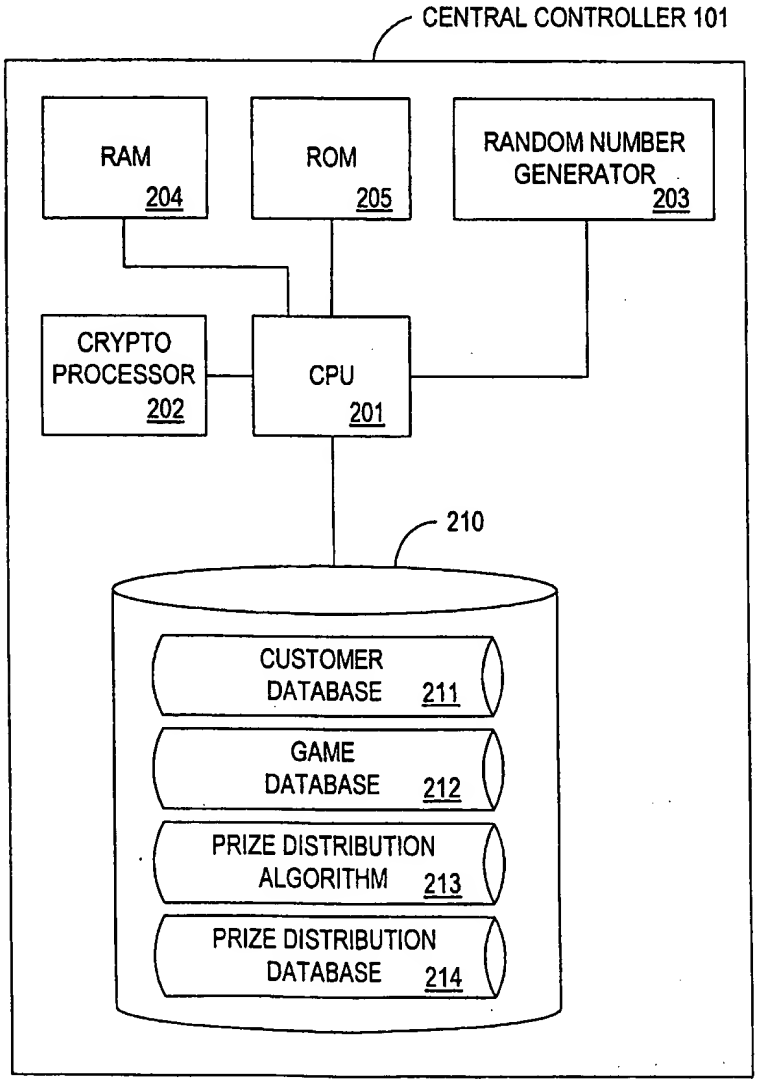

CENTRAL CONTROLLER 101
RAM
204
ROM
205
RANDOM NUMBER GENERATOR
203
CRYPTO PROCESSOR
202
CPU
201
210
CUSTOMER DATABASE
211
GAME DATABASE
212
PRIZE DISTRIBUTION ALGORITHM
213
PRIZE DISTRIBUTION DATABASE
214

FIG. 2

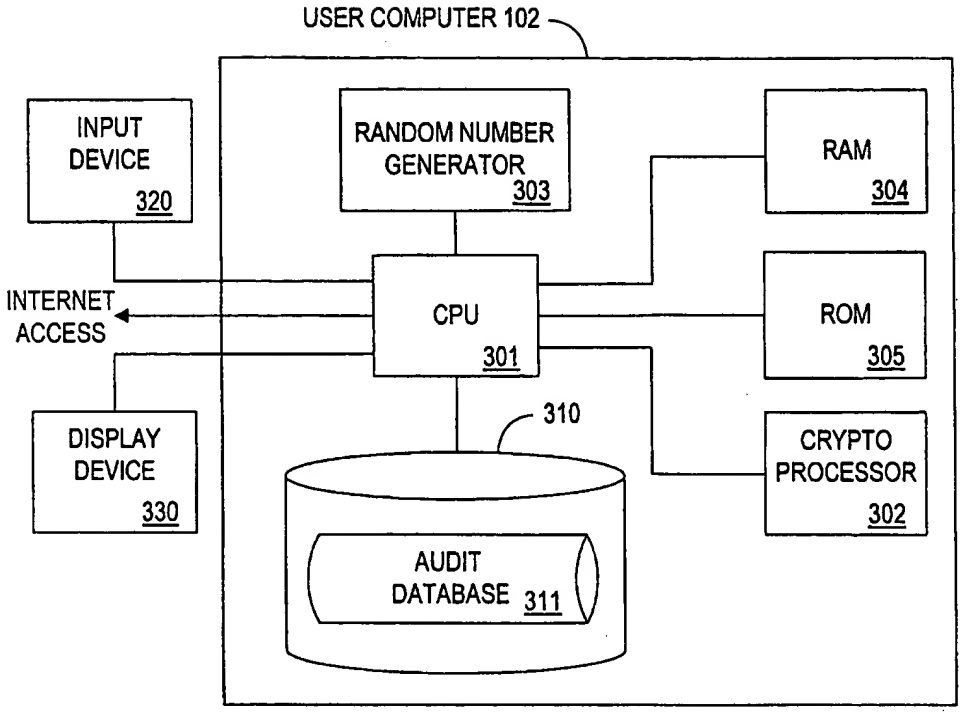

USER COMPUTER 102
INPUT DEVICE 320
RANDOM NUMBER GENERATOR 303
RAM 304
INTERNET ACCESS
CPU 301
ROM 305
310
DISPLAY DEVICE 330
CRYPTO PROCESSOR 302
AUDIT DATABASE 311

FIG. 3

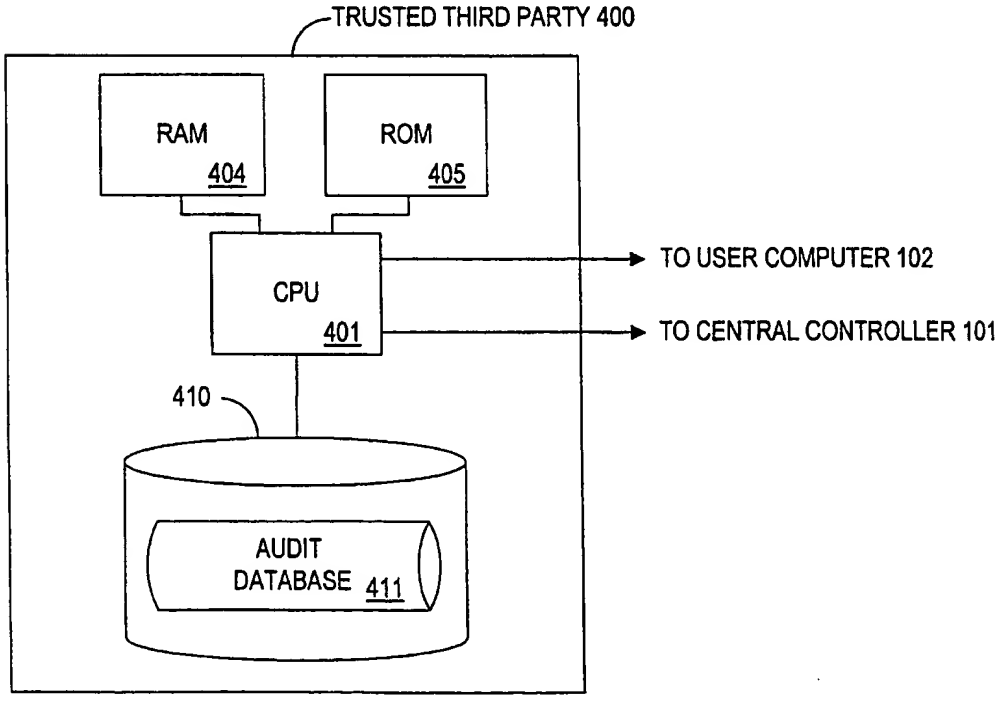

TRUSTED THIRD PARTY 400
RAM 404
ROM 405
CPU 401
TO USER COMPUTER 102
TO CENTRAL CONTROLLER 101
410
AUDIT DATABASE 411

FIG. 4

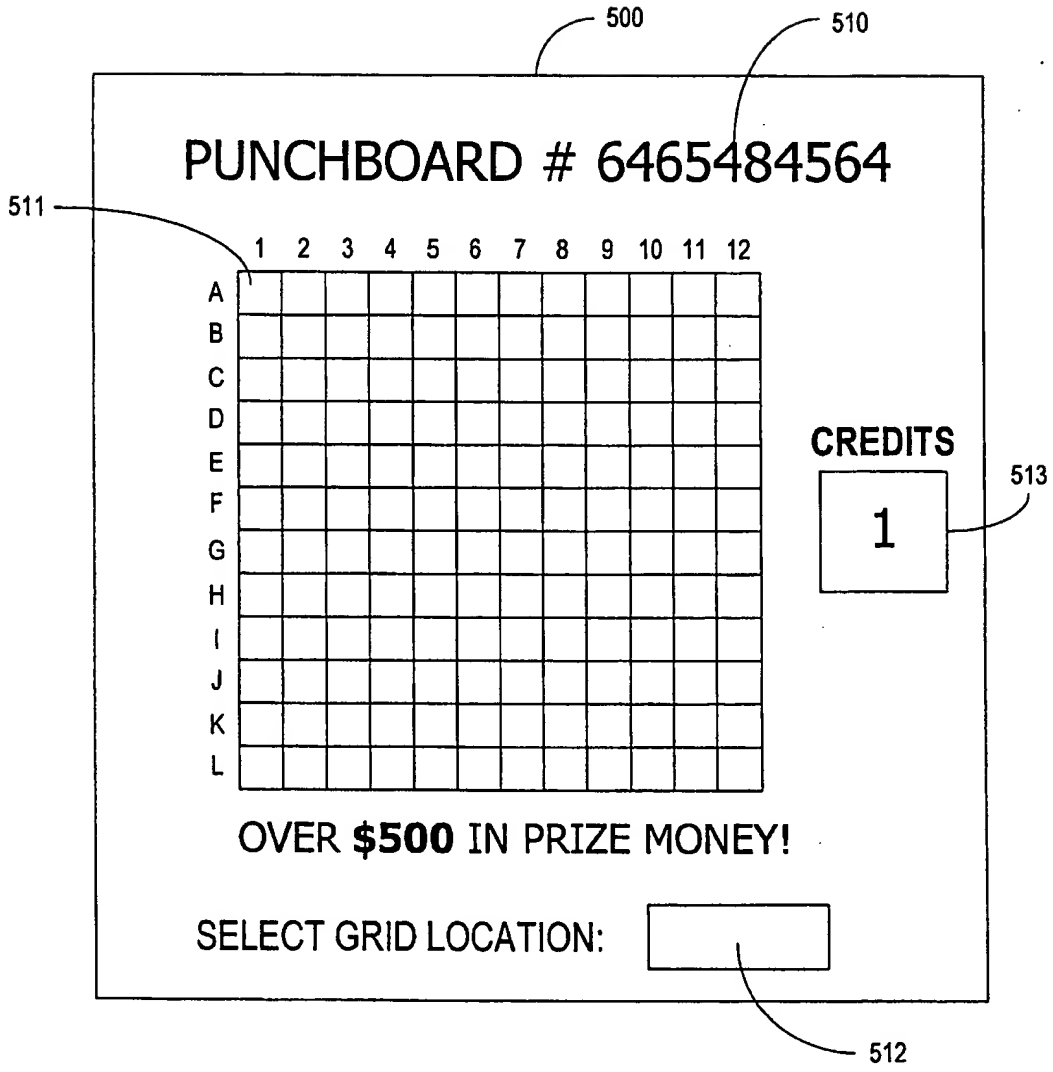

500
510
PUNCHBOARD # 6465484564
511
1 2 3 4 5 6 7 8 9 10 11 12
A
B
C
D
E
F
G
H
I
J
K
L
CREDITS
1
513
OVER $500 IN PRIZE MONEY!
SELECT GRID LOCATION:
512

FIG. 5

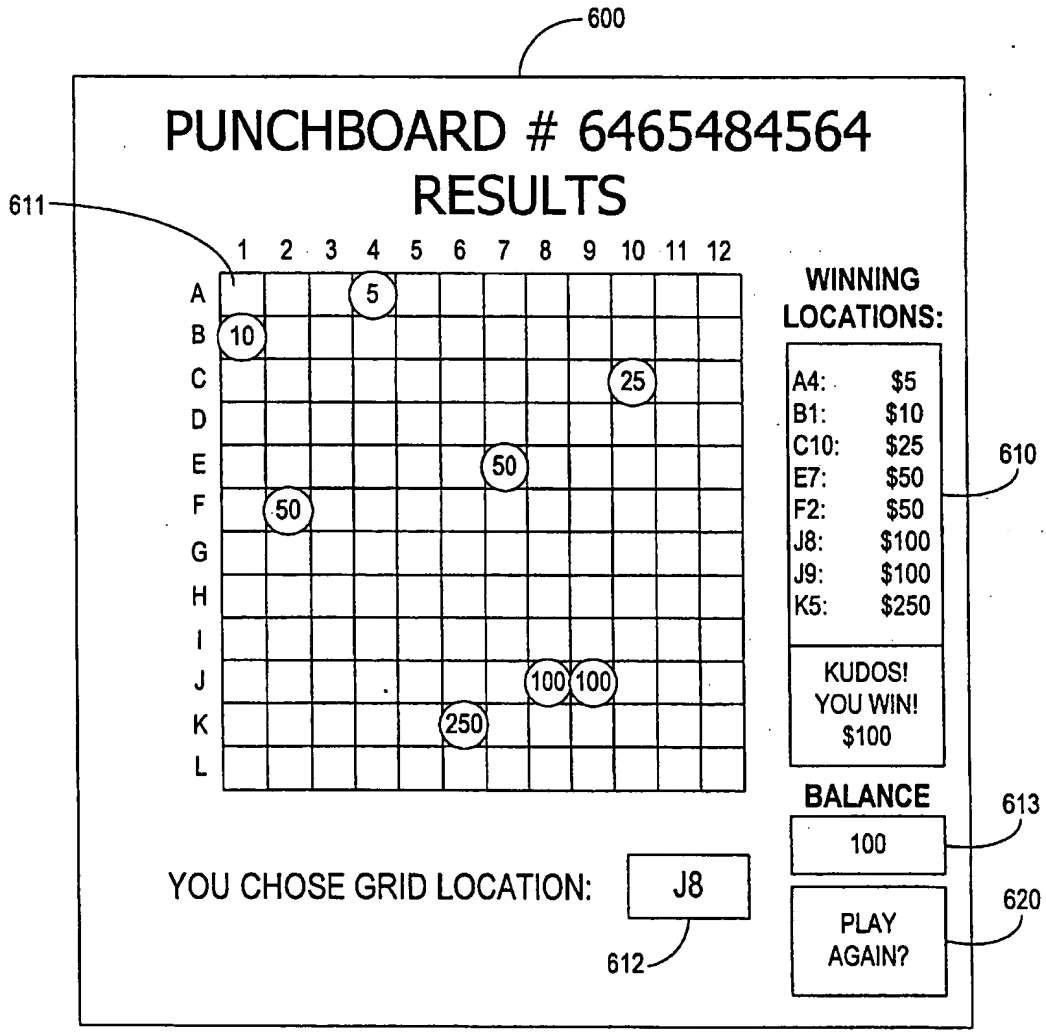

600
PUNCHBOARD # 6465484564
RESULTS
611
1 2 3 4 5 6 7 8 9 10 11 12
A
B
C
D
E
F
G
H
I
J
K
L
5
10
25
50
50
100
100
250
WINNING LOCATIONS:
A4: $5
B1: $10
C10: $25
E7: $50
F2: $50
J8: $100
J9: $100
K5: $250
610
KUDOS! YOU WIN! $100
BALANCE
613
100
YOU CHOSE GRID LOCATION:
J8
612
620
PLAY AGAIN?

FIG. 6

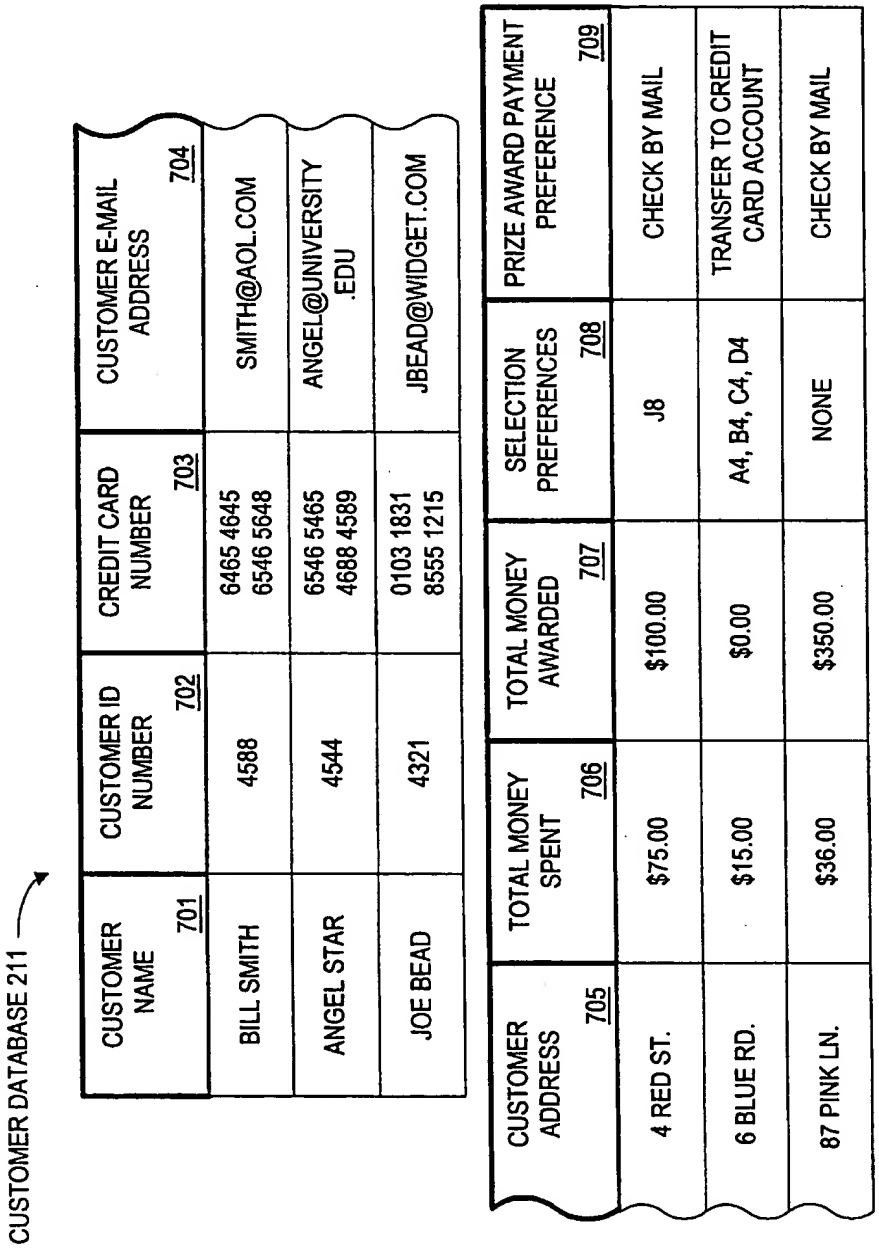

CUSTOMER DATABASE 211
CUSTOMER NAME 701
CUSTOMER ID NUMBER 702
CREDIT CARD NUMBER 703
CUSTOMER E-MAIL ADDRESS 704
BILL SMITH
4588
6465 4645 6546 5648
SMITH@AOL.COM
ANGEL STAR
4544
6546 5465 4688 4589
ANGEL@UNIVERSITY .EDU
JOE BEAD
4321
0103 1831 8555 1215
JBEAD@WIDGET.COM
CUSTOMER ADDRESS 705
TOTAL MONEY SPENT 706
TOTAL MONEY AWARDED 707
SELECTION PREFERENCES 708
PRIZE AWARD PAYMENT PREFERENCE 709
4 RED ST.
$75.00
$100.00
J8
CHECK BY MAIL
6 BLUE RD.
$15.00
$0.00
A4, B4, C4, D4
TRANSFER TO CREDIT CARD ACCOUNT
87 PINK LN.
$36.00
$350.00
NONE
CHECK BY MAIL

FIG. 7A

PRIZE DISTRIBUTION DATABASE 214

PRIZE DISTRIBUTION IDENTIFICATION NUMBER 711	GRID SIZE 712	DENOMINATION 713	PRIZE ALLOCATION 714
001	10 X 10	$1.00	$50, $5, $10, $25, $50, $100, $25, $5
002	20 X 30	$3.00	$5, $10, $25, $50, $50, $100, $100, $250
003	30 X 30	$5.00	$100, $25, $50, $100, $100, $250, $500, $5
004	30 X 30	$5.00	$1,000, $500, $500, $250, $250, $100, $100, $100, $50, $50, $50, $25, $15, $5, $5

FIG. 7B

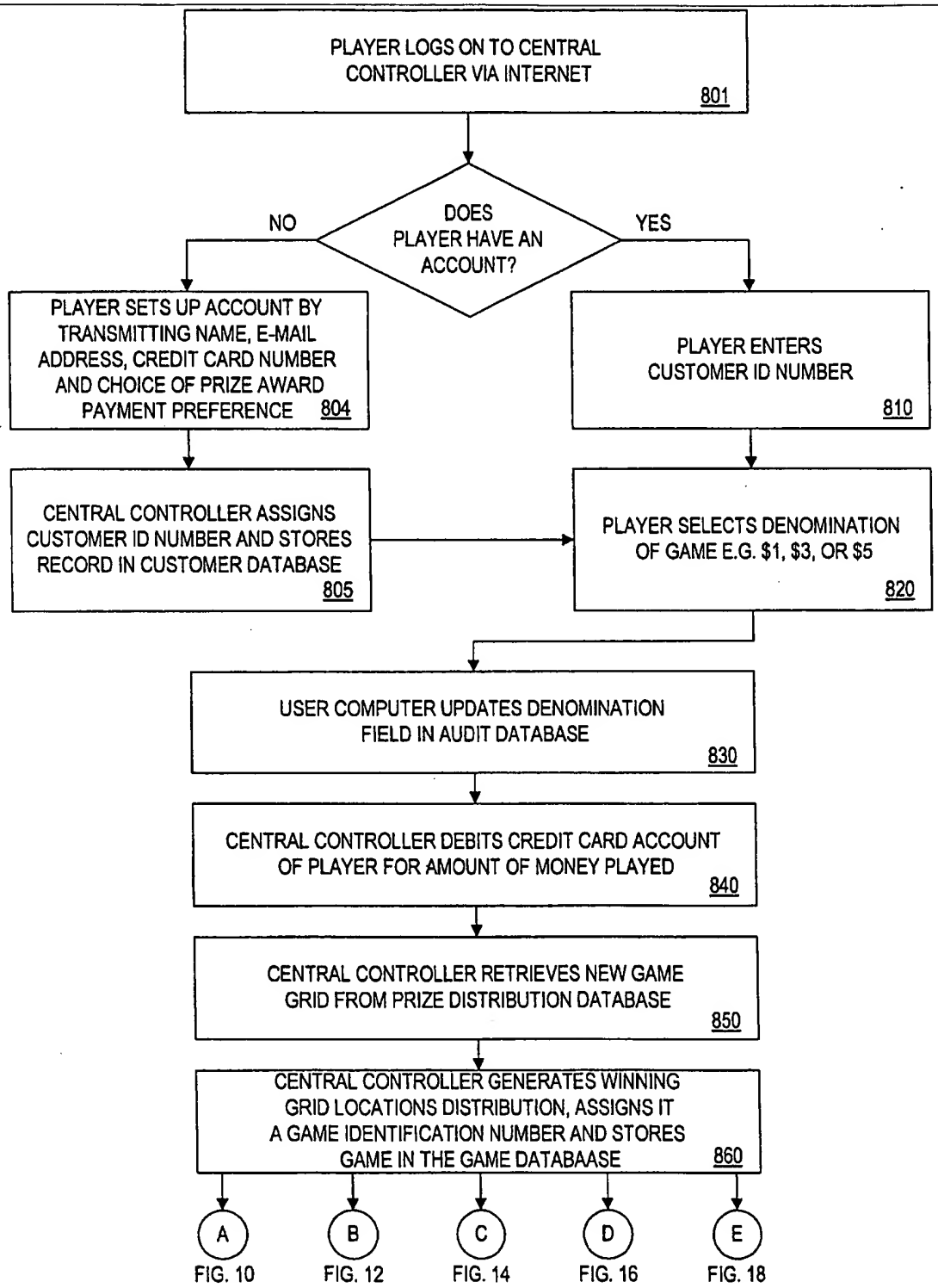

PLAYER LOGS ON TO CENTRAL CONTROLLER VIA INTERNET
801
DOES PLAYER HAVE AN ACCOUNT?
NO
YES
PLAYER SETS UP ACCOUNT BY TRANSMITTING NAME, E-MAIL ADDRESS, CREDIT CARD NUMBER AND CHOICE OF PRIZE AWARD PAYMENT PREFERENCE 804
PLAYER ENTERS CUSTOMER ID NUMBER
810
CENTRAL CONTROLLER ASSIGNS CUSTOMER ID NUMBER AND STORES RECORD IN CUSTOMER DATABASE
805
PLAYER SELECTS DENOMINATION OF GAME E.G. $1, $3, OR $5
820
USER COMPUTER UPDATES DENOMINATION FIELD IN AUDIT DATABASE
830
CENTRAL CONTROLLER DEBITS CREDIT CARD ACCOUNT OF PLAYER FOR AMOUNT OF MONEY PLAYED
840
CENTRAL CONTROLLER RETRIEVES NEW GAME GRID FROM PRIZE DISTRIBUTION DATABASE
850
CENTRAL CONTROLLER GENERATES WINNING GRID LOCATIONS DISTRIBUTION, ASSIGNS IT A GAME IDENTIFICATION NUMBER AND STORES GAME IN THE GAME DATABAASE
860
A
B
C
D
E
FIG. 10
FIG. 12
FIG. 14
FIG. 16
FIG. 18

FIG. 8

AUDIT DATABASE 311

GAME IDENTIFICATION NUMBER 901	SELECTED GRID LOCATION(S) 902	WINNING GRID LOCATIONS 903	DENOMINATION 713	PLAYER KEY 904
6465484564	J8	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	$3.00	1100010101101001011011010 11...
6465486546	A4, I2, K1	A5 $100, D7 $25, E8 $25, E9 $100, F7 $100, G3 $250, G6 $500, G7 $5	$5.00	1100011001111010110101011...
6214563168		A1 $50, C7 $5, B7 $10, E9 $50, F1 $100, G4 $25, G9 $5, H1 $25	$1.00	

FIG. 9A

GAME DATABASE 212

GAME IDENTIFICATION NUMBER 901	CUSTOMER ID NUMBER 702	WINNING GRID LOCATION 903	ENCRYPTED GRID LOCATION 910	DECRYPTED GRID LOCATION 920	PLAYER KEY 930
6465484564	4588	A4 $5, B1 $10, C 10 $25, E7 $50, J8 $100, J9 $100, K5 $250	AS498DF...	J8	10101010111011...
6465484565	4544	A2 $5, B3 $10, B4 $100, D6 $250, D7 $25, E2 $50, G1 $50	ADSFU90A8 FLDJ0D...		
	4321	A9 $100, C5 $50, D1 $100,E9 $25, F5 $25, G4 $50, G8 $25, H1 $250			
		A8 $25, B3 $50, C1 $5, D2 $10, G4 $100, H6 $250, J11 $25, K3 $100			

FIG. 9B

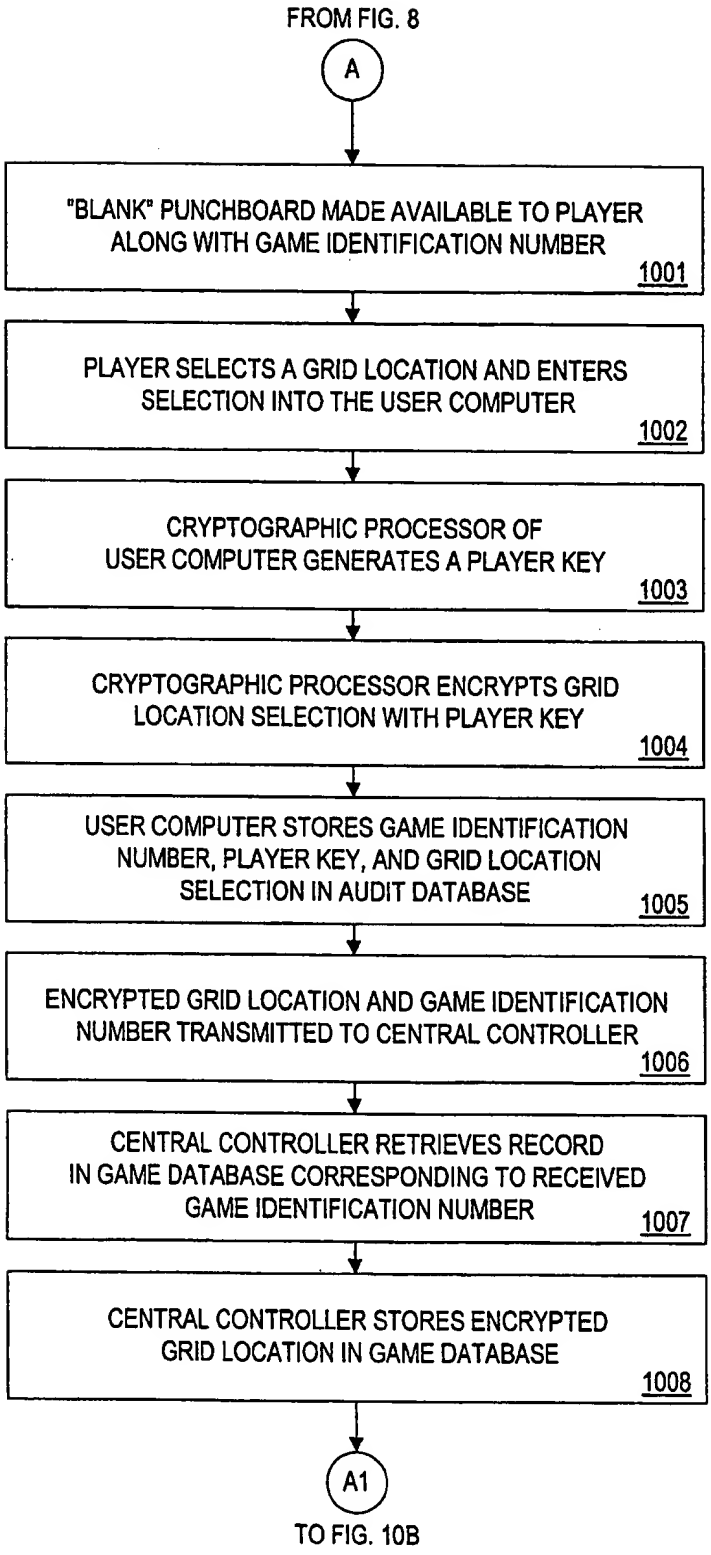

FROM FIG. 8
A
"BLANK" PUNCHBOARD MADE AVAILABLE TO PLAYER ALONG WITH GAME IDENTIFICATION NUMBER
1001
PLAYER SELECTS A GRID LOCATION AND ENTERS SELECTION INTO THE USER COMPUTER
1002
CRYPTOGRAPHIC PROCESSOR OF USER COMPUTER GENERATES A PLAYER KEY
1003
CRYPTOGRAPHIC PROCESSOR ENCRYPTS GRID LOCATION SELECTION WITH PLAYER KEY
1004
USER COMPUTER STORES GAME IDENTIFICATION NUMBER, PLAYER KEY, AND GRID LOCATION SELECTION IN AUDIT DATABASE
1005
ENCRYPTED GRID LOCATION AND GAME IDENTIFICATION NUMBER TRANSMITTED TO CENTRAL CONTROLLER
1006
CENTRAL CONTROLLER RETRIEVES RECORD IN GAME DATABASE CORRESPONDING TO RECEIVED GAME IDENTIFICATION NUMBER
1007
CENTRAL CONTROLLER STORES ENCRYPTED GRID LOCATION IN GAME DATABASE
1008
A1
TO FIG. 10B

FIG. 10A

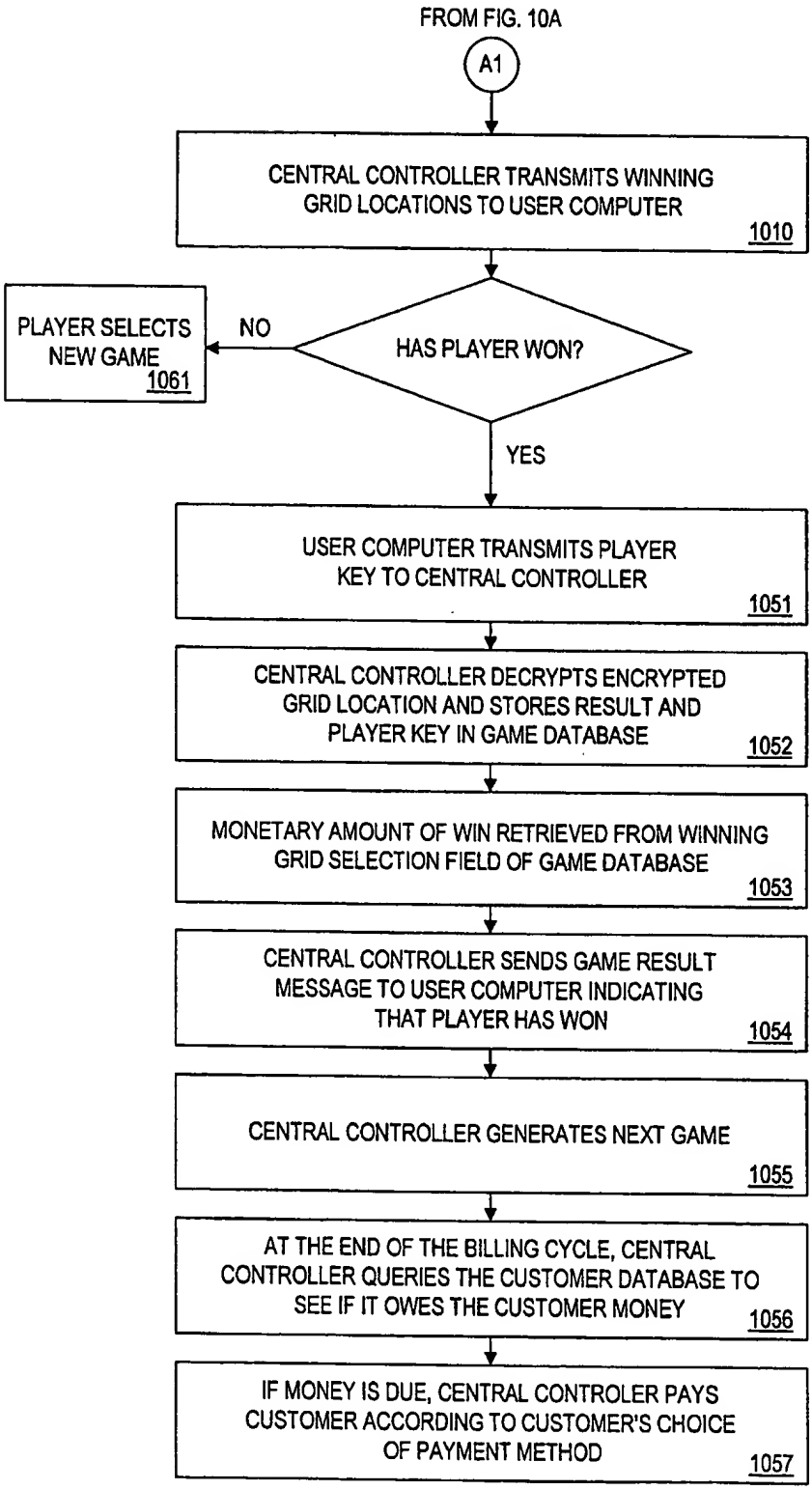

FROM FIG. 10A
A1
CENTRAL CONTROLLER TRANSMITS WINNING GRID LOCATIONS TO USER COMPUTER
1010
HAS PLAYER WON?
NO
PLAYER SELECTS NEW GAME
1061
YES
USER COMPUTER TRANSMITS PLAYER KEY TO CENTRAL CONTROLLER
1051
CENTRAL CONTROLLER DECRYPTS ENCRYPTED GRID LOCATION AND STORES RESULT AND PLAYER KEY IN GAME DATABASE
1052
MONETARY AMOUNT OF WIN RETRIEVED FROM WINNING GRID SELECTION FIELD OF GAME DATABASE
1053
CENTRAL CONTROLLER SENDS GAME RESULT MESSAGE TO USER COMPUTER INDICATING THAT PLAYER HAS WON
1054
CENTRAL CONTROLLER GENERATES NEXT GAME
1055
AT THE END OF THE BILLING CYCLE, CENTRAL CONTROLLER QUERIES THE CUSTOMER DATABASE TO SEE IF IT OWES THE CUSTOMER MONEY
1056
IF MONEY IS DUE, CENTRAL CONTROLER PAYS CUSTOMER ACCORDING TO CUSTOMER'S CHOICE OF PAYMENT METHOD
1057

FIG. 10B

AUDIT DATABASE 311

GAME IDENTIFICATION NUMBER 901	SELECTED GRID LOCATION 902	WINNING GRID LOCATIONS 903	DENOMINATION 713	HASH OF WINNING GRID LOCATIONS 1101
6465484564	J8	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	$3.00	101000011101 1011010111...
6465486546	A4, I2, K1		$5.00	101010111110 10110110101...
6215467168			$1.00	101001101011 10101101011...
6215463175			$3.00	

FIG. 11A

GAME DATABASE 212

GAME IDENTIFICATION NUMBER 901	CUSTOMER ID NUMBER 702	WINNING GRID LOCATIONS 903	USER GRID SELECTION 902	HASH OF WINNING GRID LOCATION 1101
6465484564	4588	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	J8	101000111010...
6465484565	4544	A2 $5, B3 $10, B4 $100, D6 $250, D7 $25, E2 $50, G1 $50		101010111110...
64654845666	4321	A9 $100, C5 $50, D1 $100, E9 $25, F5 $25, G4 $50, G8 $25, H1 $250		
64654845667		A8, $25, B3 $$50, C1 $5, D2 $10, G4 $100,H6 $250, J11, $25, K3 $100		

FIG. 11B

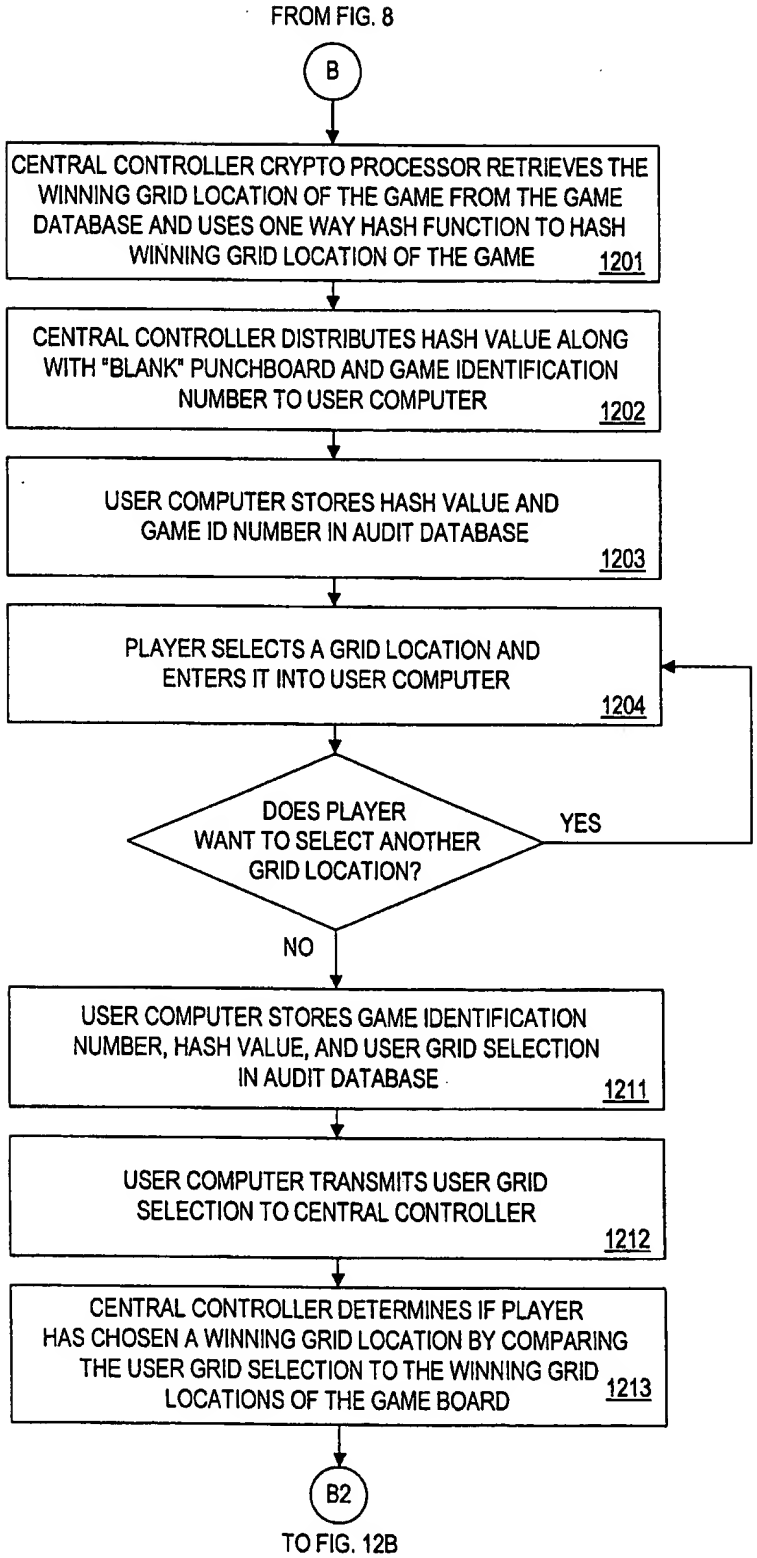

FROM FIG. 8
B
CENTRAL CONTROLLER CRYPTO PROCESSOR RETRIEVES THE WINNING GRID LOCATION OF THE GAME FROM THE GAME DATABASE AND USES ONE WAY HASH FUNCTION TO HASH WINNING GRID LOCATION OF THE GAME 1201
CENTRAL CONTROLLER DISTRIBUTES HASH VALUE ALONG WITH "BLANK" PUNCHBOARD AND GAME IDENTIFICATION NUMBER TO USER COMPUTER 1202
USER COMPUTER STORES HASH VALUE AND GAME ID NUMBER IN AUDIT DATABASE 1203
PLAYER SELECTS A GRID LOCATION AND ENTERS IT INTO USER COMPUTER 1204
DOES PLAYER WANT TO SELECT ANOTHER GRID LOCATION?
YES
NO
USER COMPUTER STORES GAME IDENTIFICATION NUMBER, HASH VALUE, AND USER GRID SELECTION IN AUDIT DATABASE 1211
USER COMPUTER TRANSMITS USER GRID SELECTION TO CENTRAL CONTROLLER 1212
CENTRAL CONTROLLER DETERMINES IF PLAYER HAS CHOSEN A WINNING GRID LOCATION BY COMPARING THE USER GRID SELECTION TO THE WINNING GRID LOCATIONS OF THE GAME BOARD 1213
B2
TO FIG. 12B

FIG. 12A

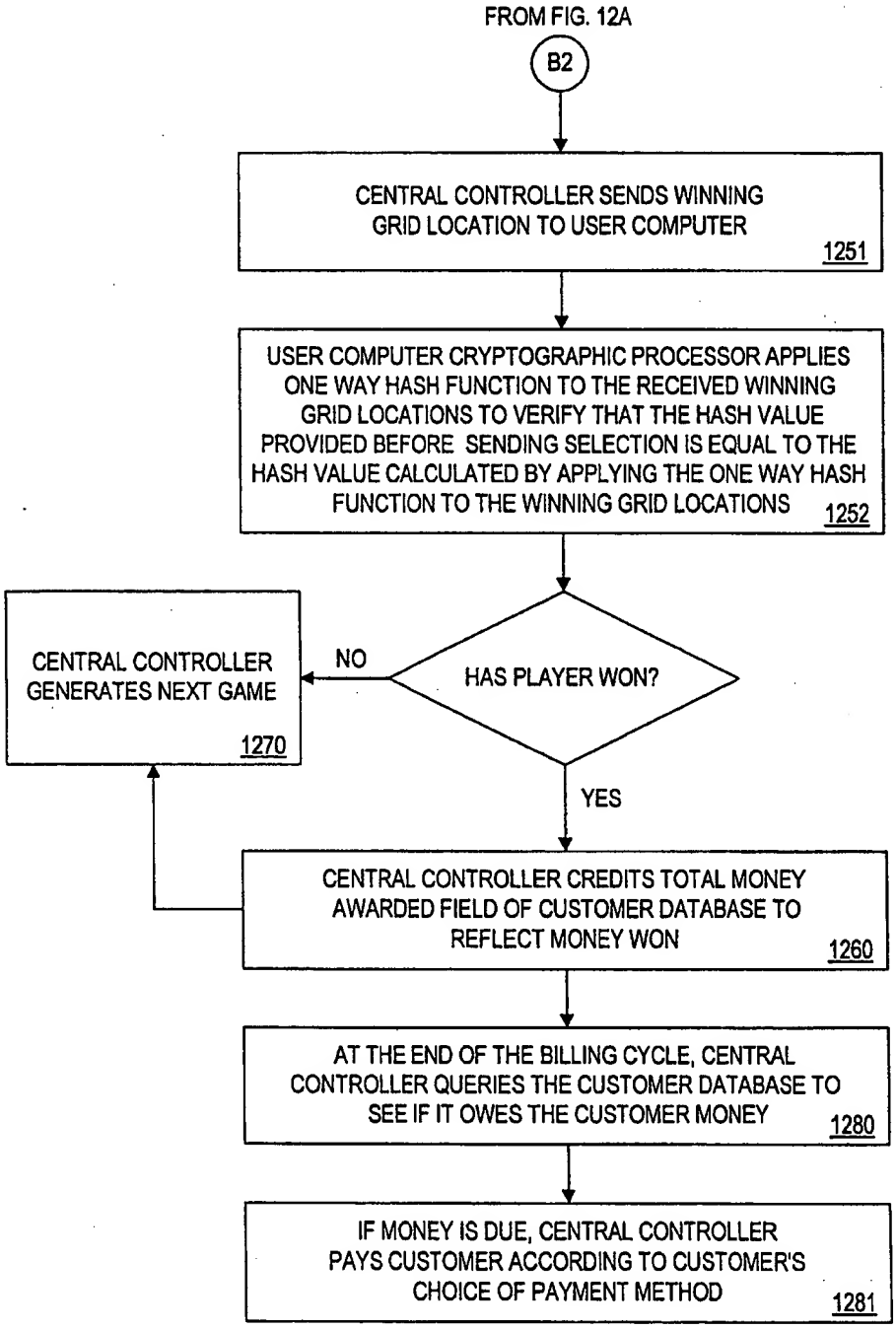

FROM FIG. 12A
B2
CENTRAL CONTROLLER SENDS WINNING GRID LOCATION TO USER COMPUTER
1251
USER COMPUTER CRYPTOGRAPHIC PROCESSOR APPLIES ONE WAY HASH FUNCTION TO THE RECEIVED WINNING GRID LOCATIONS TO VERIFY THAT THE HASH VALUE PROVIDED BEFORE SENDING SELECTION IS EQUAL TO THE HASH VALUE CALCULATED BY APPLYING THE ONE WAY HASH FUNCTION TO THE WINNING GRID LOCATIONS
1252
HAS PLAYER WON?
NO
CENTRAL CONTROLLER GENERATES NEXT GAME
1270
YES
CENTRAL CONTROLLER CREDITS TOTAL MONEY AWARDED FIELD OF CUSTOMER DATABASE TO REFLECT MONEY WON
1260
AT THE END OF THE BILLING CYCLE, CENTRAL CONTROLLER QUERIES THE CUSTOMER DATABASE TO SEE IF IT OWES THE CUSTOMER MONEY
1280
IF MONEY IS DUE, CENTRAL CONTROLLER PAYS CUSTOMER ACCORDING TO CUSTOMER'S CHOICE OF PAYMENT METHOD
1281

FIG. 12B

AUDIT DATABASE 311

GAME IDENTIFICATION NUMBER 901	SELECTED GRID LOCATION 902	WINNING GRID LOCATIONS 903	DENOMINATION 713	HASH VALUE OF ALL GRID LOCATIONS 1101	AGGREGATE HASH VALUE 1301
6465484564	J8	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	$3.00	101000011101 1011010111...	101001000100 0111101011...
6465486546	A4, I2, K1		$5.00	1010101111101 0110110101...	
6215467168			$1.00	101001101011 10101101011...	
621543175			$3.00		

FIG. 13A

GAME DATABASE 212

GAME IDENTIFICATION NUMBER 901	CUSTOMER ID NUMBER 702	WINNING GRID LOCATIONS 903	USER SELECTED GRID LOCATIONS 902	HASH VALUE OF ENTIRE GRID 1101	AGGREGATE HASH VALUE 1301	DENOMINATION 713
6465484564	4588	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	J8	101000111010...	10100100010 0110011110...	$3.00
6465484564	4589	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	C2	101010111110...	10100000111 1101110000...	$3.00
6465484564	3218	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	C12, D13	101001101011...		$3.00
6465484564		A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250				$3.00

FIG. 13B

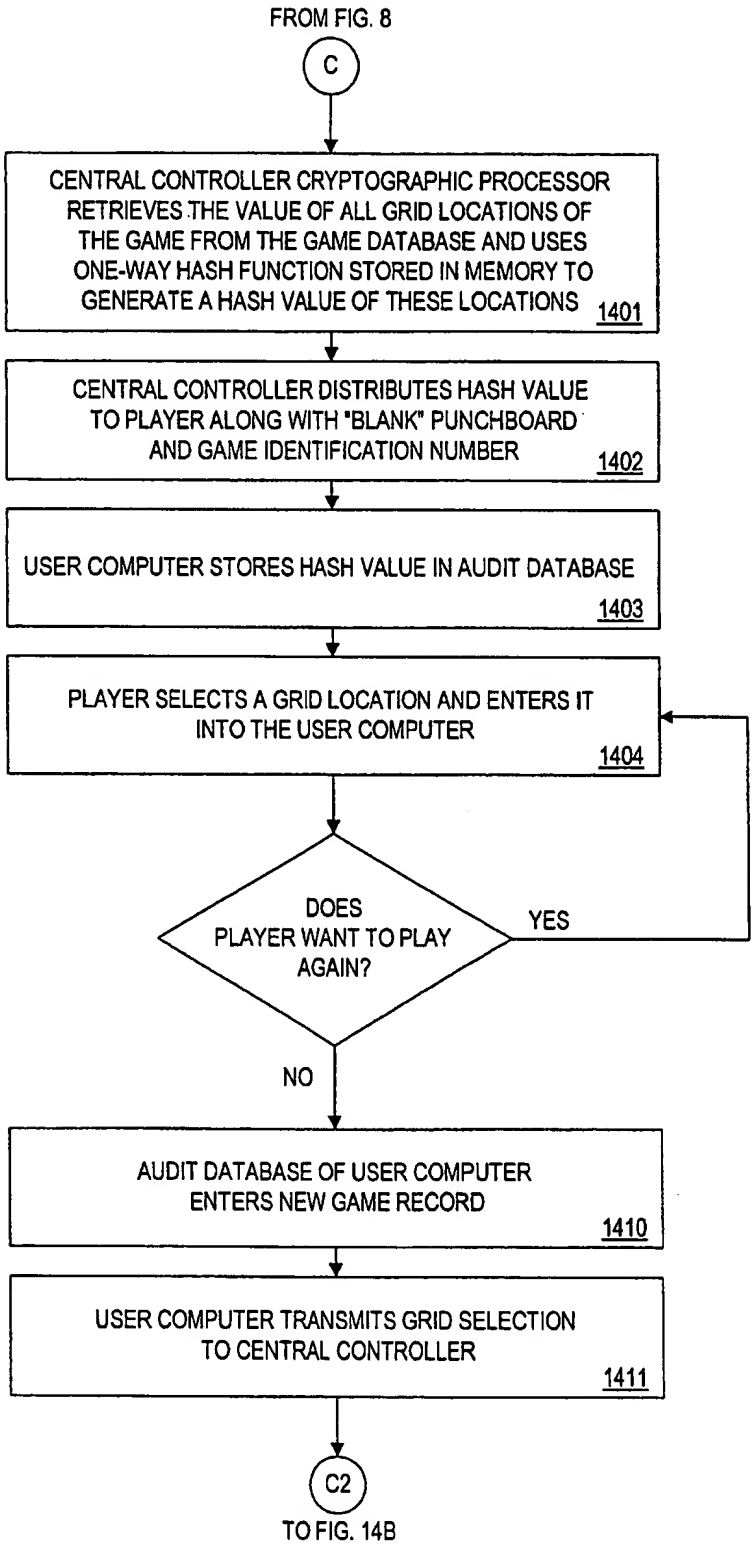

FROM FIG. 8
C
CENTRAL CONTROLLER CRYPTOGRAPHIC PROCESSOR RETRIEVES THE VALUE OF ALL GRID LOCATIONS OF THE GAME FROM THE GAME DATABASE AND USES ONE-WAY HASH FUNCTION STORED IN MEMORY TO GENERATE A HASH VALUE OF THESE LOCATIONS 1401
CENTRAL CONTROLLER DISTRIBUTES HASH VALUE TO PLAYER ALONG WITH "BLANK" PUNCHBOARD AND GAME IDENTIFICATION NUMBER 1402
USER COMPUTER STORES HASH VALUE IN AUDIT DATABASE 1403
PLAYER SELECTS A GRID LOCATION AND ENTERS IT INTO THE USER COMPUTER 1404
DOES PLAYER WANT TO PLAY AGAIN?
YES
NO
AUDIT DATABASE OF USER COMPUTER ENTERS NEW GAME RECORD 1410
USER COMPUTER TRANSMITS GRID SELECTION TO CENTRAL CONTROLLER 1411
C2
TO FIG. 14B

FIG. 14A

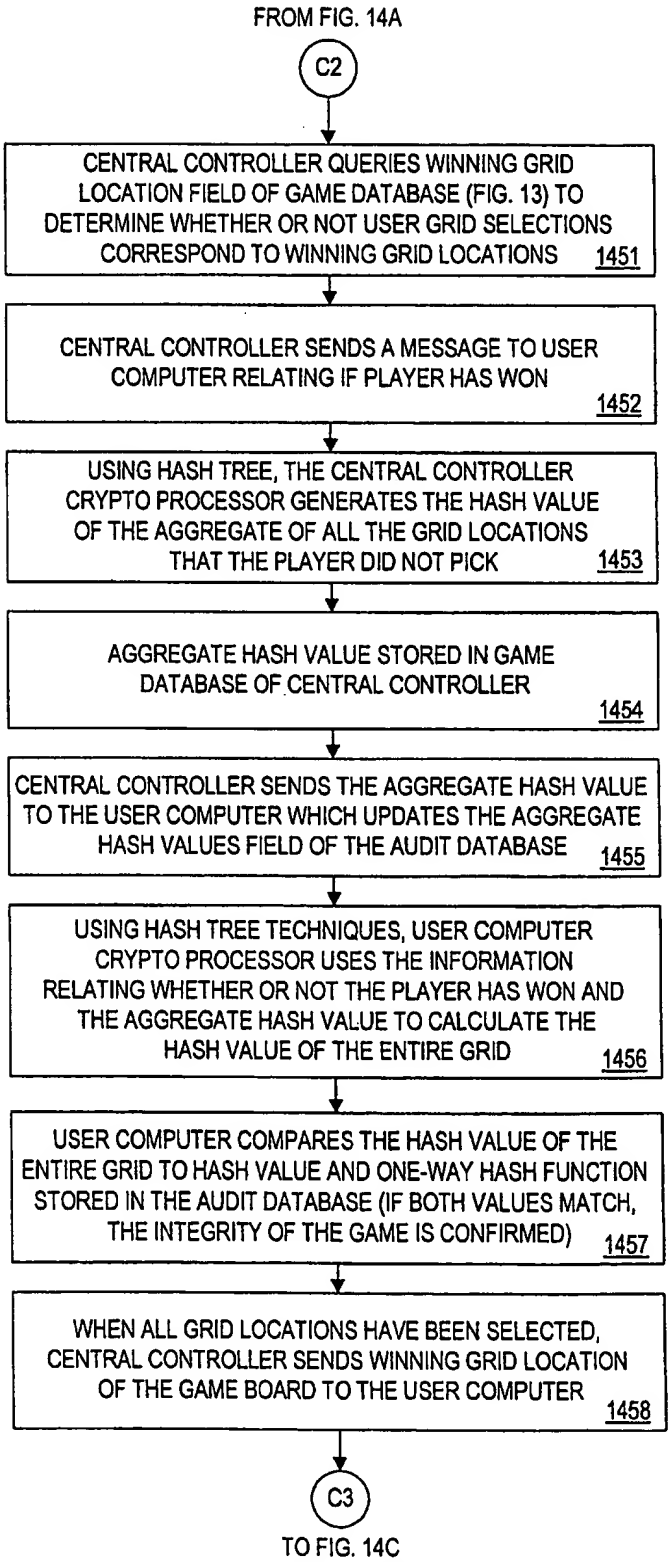

FROM FIG. 14A
C2
CENTRAL CONTROLLER QUERIES WINNING GRID LOCATION FIELD OF GAME DATABASE (FIG. 13) TO DETERMINE WHETHER OR NOT USER GRID SELECTIONS CORRESPOND TO WINNING GRID LOCATIONS 1451
CENTRAL CONTROLLER SENDS A MESSAGE TO USER COMPUTER RELATING IF PLAYER HAS WON 1452
USING HASH TREE, THE CENTRAL CONTROLLER CRYPTO PROCESSOR GENERATES THE HASH VALUE OF THE AGGREGATE OF ALL THE GRID LOCATIONS THAT THE PLAYER DID NOT PICK 1453
AGGREGATE HASH VALUE STORED IN GAME DATABASE OF CENTRAL CONTROLLER 1454
CENTRAL CONTROLLER SENDS THE AGGREGATE HASH VALUE TO THE USER COMPUTER WHICH UPDATES THE AGGREGATE HASH VALUES FIELD OF THE AUDIT DATABASE 1455
USING HASH TREE TECHNIQUES, USER COMPUTER CRYPTO PROCESSOR USES THE INFORMATION RELATING WHETHER OR NOT THE PLAYER HAS WON AND THE AGGREGATE HASH VALUE TO CALCULATE THE HASH VALUE OF THE ENTIRE GRID 1456
USER COMPUTER COMPARES THE HASH VALUE OF THE ENTIRE GRID TO HASH VALUE AND ONE-WAY HASH FUNCTION STORED IN THE AUDIT DATABASE (IF BOTH VALUES MATCH, THE INTEGRITY OF THE GAME IS CONFIRMED) 1457
WHEN ALL GRID LOCATIONS HAVE BEEN SELECTED, CENTRAL CONTROLLER SENDS WINNING GRID LOCATION OF THE GAME BOARD TO THE USER COMPUTER 1458
C3
TO FIG. 14C

FIG. 14B

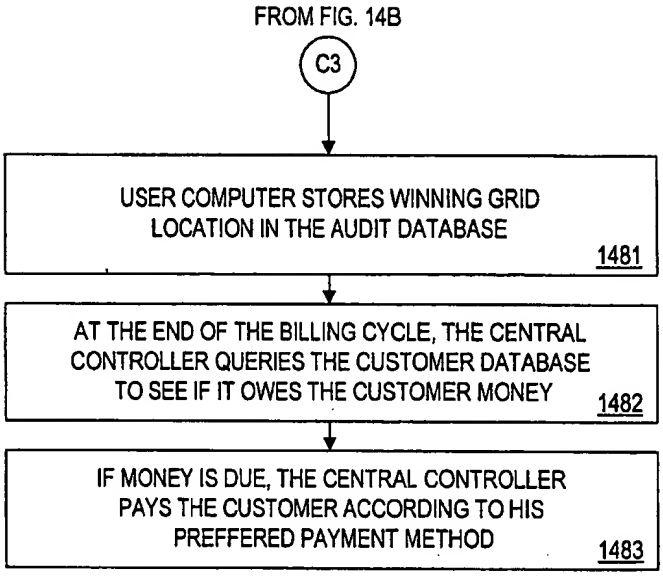

FROM FIG. 14B
C3
USER COMPUTER STORES WINNING GRID LOCATION IN THE AUDIT DATABASE
1481
AT THE END OF THE BILLING CYCLE, THE CENTRAL CONTROLLER QUERIES THE CUSTOMER DATABASE TO SEE IF IT OWES THE CUSTOMER MONEY
1482
IF MONEY IS DUE, THE CENTRAL CONTROLLER PAYS THE CUSTOMER ACCORDING TO HIS PREFFERED PAYMENT METHOD
1483

FIG. 14C

AUDIT DATABASE 311

GAME IDENTIFICATION NUMBER 901	SELECTED GRID LOCATION 902	DECRYPTED WINNING GRID LOCATIONS 1530	ENCRYPTED WINNING GRID LOCATIONS 1520	DENOMINATION 713	RANDOM KEY 1510
6465484564	J8	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	001011010110011	$3.00	1100010101101 00110101011...
6564486546	A4, I2, K1	A5 $100, D7 $25, E8 $50, E9 $100, F7 $100, G3 $250, G6 $500, G7 $5	101011001100111	$5.00	1100011001111 01011010101...
6215463168		A1 $50, C7 $5, B7 $10, E9 $50, F1 $100, G4 $25, G9 $5, H1 $25	111011001100111	$1.00	
				$3.00	

FIG. 15A

GAME DATABASE 212

GAME IDENTIFICATION NUMBER 901	CUSTOMER ID NUMBER 702	WINNING GRID LOCATIONS 903	USER SELECTED GRID LOCATION 902	RANDOM KEY 1510	DENOMINATION OF GAME 713
6465484564	4588	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	J8	110001010110 100110101011...	$3.00
6465484565	4544	A2 $5, B3 $10, B4 $100, D6 $250, D7 $25 E2 $50, G1 $50	A4, I2, K1	110001100111 101011010101...	$5.00
	4321	A9 $100, C5 $50, D1 $100, E9 $25, F5 $25, G4 $50, G8 $25, H1 $250			
		A8 $25, B3 $50, C1 $5, D2 $10, G4 $100, H6 $250, J11 $25, K3 $100			

FIG. 15B

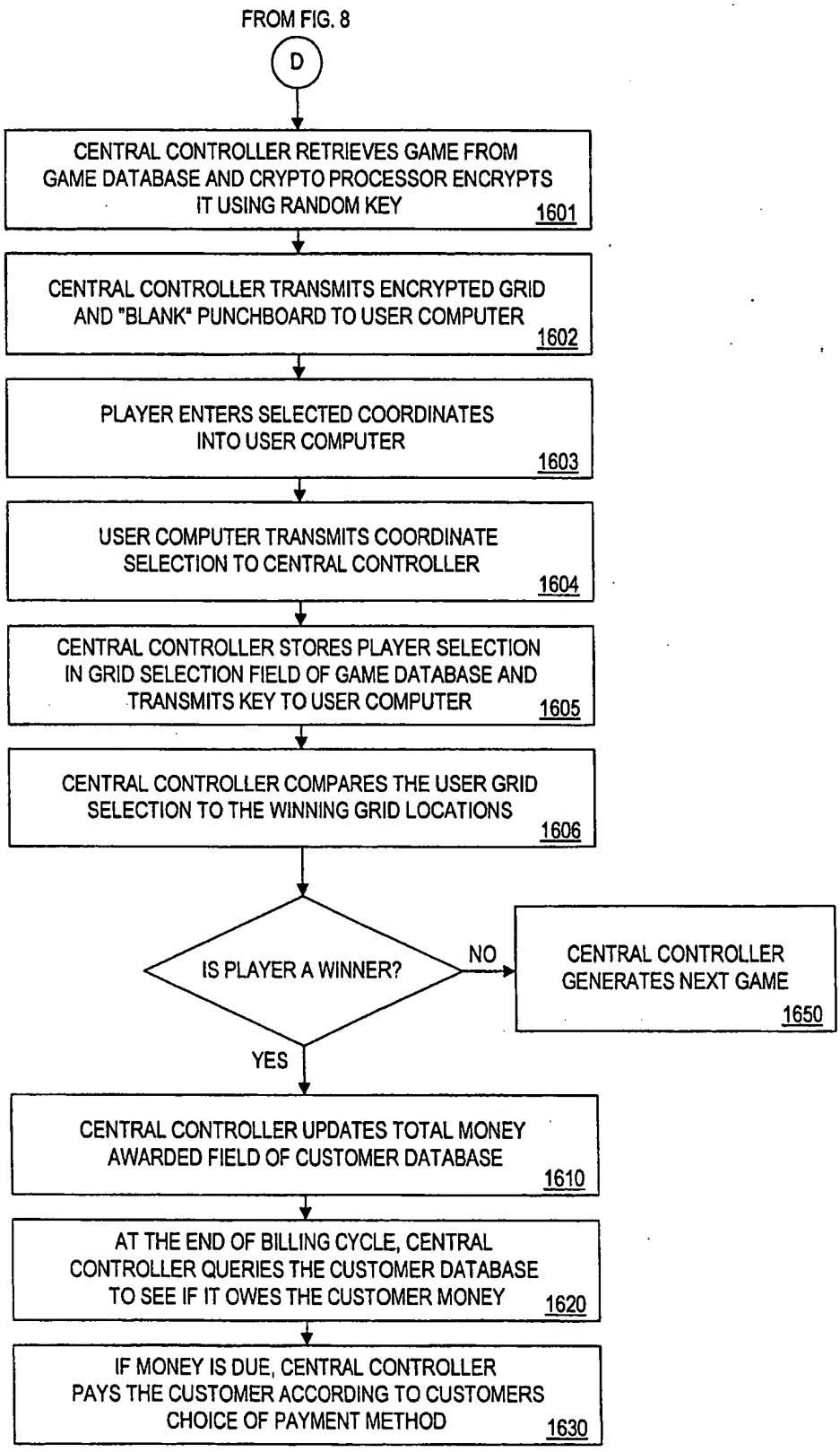

FROM FIG. 8
D
CENTRAL CONTROLLER RETRIEVES GAME FROM GAME DATABASE AND CRYPTO PROCESSOR ENCRYPTS IT USING RANDOM KEY 1601
CENTRAL CONTROLLER TRANSMITS ENCRYPTED GRID AND "BLANK" PUNCHBOARD TO USER COMPUTER 1602
PLAYER ENTERS SELECTED COORDINATES INTO USER COMPUTER 1603
USER COMPUTER TRANSMITS COORDINATE SELECTION TO CENTRAL CONTROLLER 1604
CENTRAL CONTROLLER STORES PLAYER SELECTION IN GRID SELECTION FIELD OF GAME DATABASE AND TRANSMITS KEY TO USER COMPUTER 1605
CENTRAL CONTROLLER COMPARES THE USER GRID SELECTION TO THE WINNING GRID LOCATIONS 1606
IS PLAYER A WINNER?
NO
CENTRAL CONTROLLER GENERATES NEXT GAME 1650
YES
CENTRAL CONTROLLER UPDATES TOTAL MONEY AWARDED FIELD OF CUSTOMER DATABASE 1610
AT THE END OF BILLING CYCLE, CENTRAL CONTROLLER QUERIES THE CUSTOMER DATABASE TO SEE IF IT OWES THE CUSTOMER MONEY 1620
IF MONEY IS DUE, CENTRAL CONTROLLER PAYS THE CUSTOMER ACCORDING TO CUSTOMERS CHOICE OF PAYMENT METHOD 1630

FIG. 16

AUDIT DATABASE 311

GAME IDENTIFICATION NUMBER 901	SELECTED GRID LOCATION 902	WINNING GRID LOCATIONS 903	DENOMINATION 713	CUSTOMER ID NUMBER 702
6465484564	J8	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	$1.00	4588
6465484565	A4, I2, K1	A5 $100, D7 $25, E8 $50, E9 $100, F7 $100, G3 $250, G6 $500, G7 $5	$3.00	4544
6465484566		A1 $50, C7 $5, B7 $10, E9 $50, F1 $100, G4 $25, G9 $5, H1 $25	$5.00	4321

FIG. 17A

GAME DATABASE 212

GAME IDENTIFICATION NUMBER 901	SELECTED GRID LOCATION 902	WINNING GRID LOCATIONS 903	DENOMINATION 713	CUSTOMER ID NUMBER 702
6465484564	J8	A4 $5, B1 $10, C10 $25, E7 $50, F2 $50, J8 $100, J9 $100, K5 $250	$1.00	4588
6465484565	A4, I2, K1	A5 $100, D7 $25, E8 $50, E9 $100, F7 $100, G3 $250, G6 $500, G7 $5	$3.00	4544
6465484566		A1 $50, C7 $5, B7 $10, E9 $50, F1 $100, G4 $25, G9 $5, H1 $25	$5.00	4321

FIG. 17B

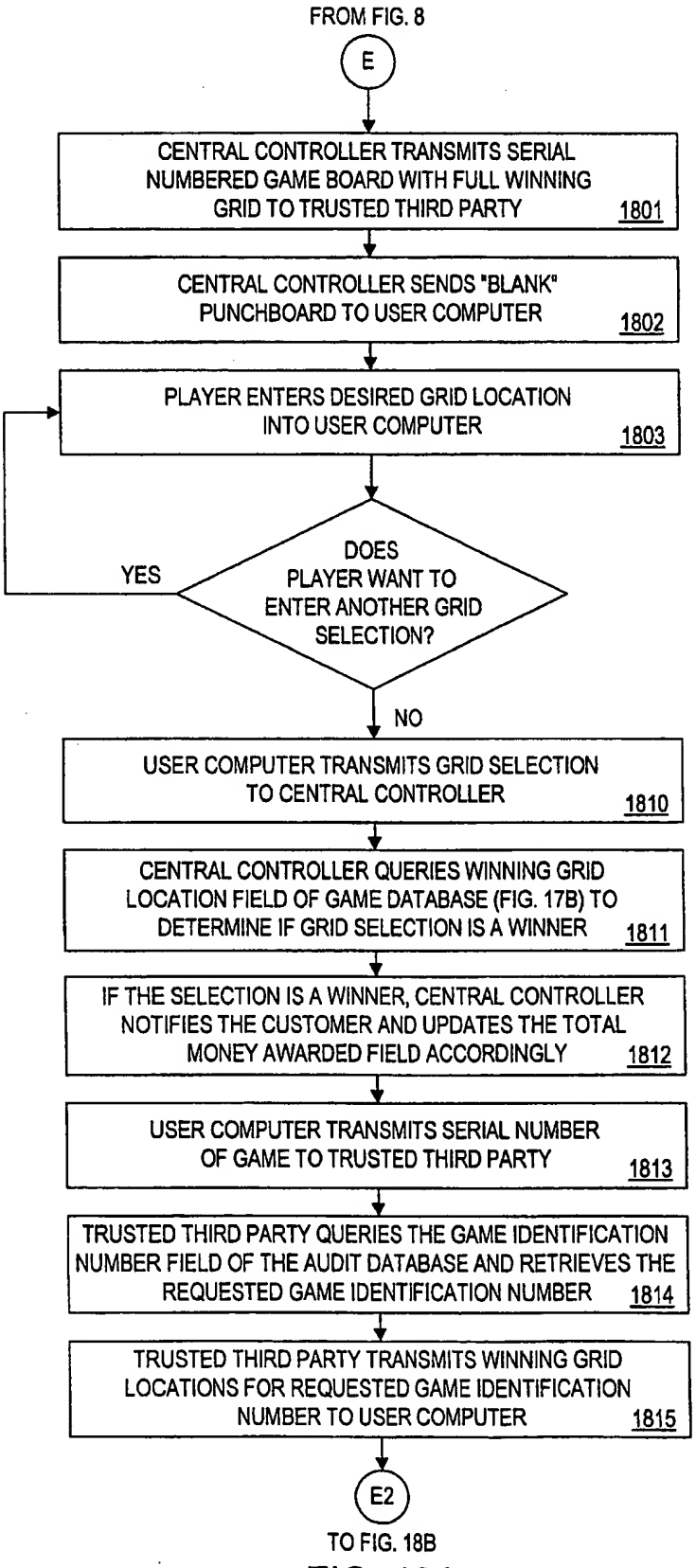

FROM FIG. 8
E
CENTRAL CONTROLLER TRANSMITS SERIAL NUMBERED GAME BOARD WITH FULL WINNING GRID TO TRUSTED THIRD PARTY 1801
CENTRAL CONTROLLER SENDS "BLANK" PUNCHBOARD TO USER COMPUTER 1802
PLAYER ENTERS DESIRED GRID LOCATION INTO USER COMPUTER 1803
DOES PLAYER WANT TO ENTER ANOTHER GRID SELECTION?
YES
NO
USER COMPUTER TRANSMITS GRID SELECTION TO CENTRAL CONTROLLER 1810
CENTRAL CONTROLLER QUERIES WINNING GRID LOCATION FIELD OF GAME DATABASE (FIG. 17B) TO DETERMINE IF GRID SELECTION IS A WINNER 1811
IF THE SELECTION IS A WINNER, CENTRAL CONTROLLER NOTIFIES THE CUSTOMER AND UPDATES THE TOTAL MONEY AWARDED FIELD ACCORDINGLY 1812
USER COMPUTER TRANSMITS SERIAL NUMBER OF GAME TO TRUSTED THIRD PARTY 1813
TRUSTED THIRD PARTY QUERIES THE GAME IDENTIFICATION NUMBER FIELD OF THE AUDIT DATABASE AND RETRIEVES THE REQUESTED GAME IDENTIFICATION NUMBER 1814
TRUSTED THIRD PARTY TRANSMITS WINNING GRID LOCATIONS FOR REQUESTED GAME IDENTIFICATION NUMBER TO USER COMPUTER 1815
E2
TO FIG. 18B

FIG. 18A

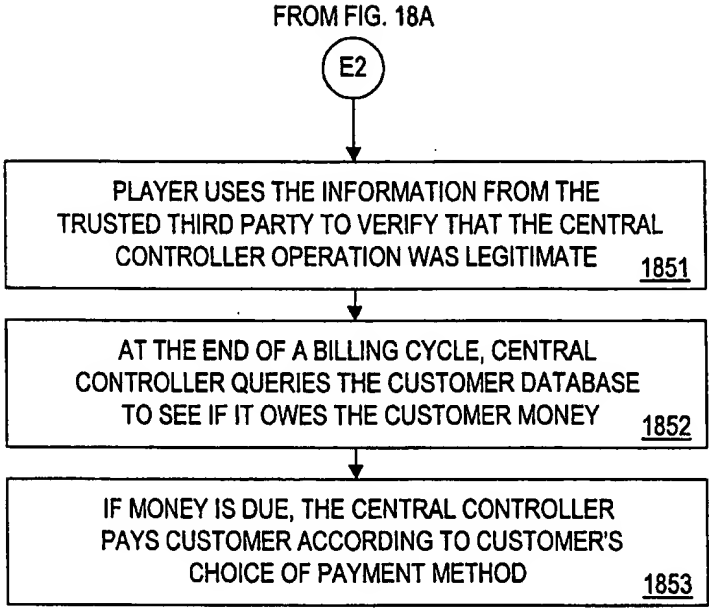

FROM FIG. 18A
E2
PLAYER USES THE INFORMATION FROM THE TRUSTED THIRD PARTY TO VERIFY THAT THE CENTRAL CONTROLLER OPERATION WAS LEGITIMATE
1851
AT THE END OF A BILLING CYCLE, CENTRAL CONTROLLER QUERIES THE CUSTOMER DATABASE TO SEE IF IT OWES THE CUSTOMER MONEY
1852
IF MONEY IS DUE, THE CENTRAL CONTROLLER PAYS CUSTOMER ACCORDING TO CUSTOMER'S CHOICE OF PAYMENT METHOD
1853

FIG. 18B